Política de Segurança da Informação

Código	PL 04
Versão	05
Área Responsável	Segurança da Informação
Aprovação	Reunião de Dir. Executiva
Expedição	30/07/2021
Nº Ata	015/2021

Sumário

1. OBJETIVO

A Política de Segurança da Informação tem como objetivo definir as diretrizes e responsabilidades que norteiam a proteção dos ativos de informação do Grupo Warren ("Warren"), estabelecendo normas e procedimentos para o Sistema de Gestão de Segurança da Informação, visando preservar a confidencialidade, integridade e disponibilidade das informações.

2. ABRANGÊNCIA

Esta política destina-se a todas as áreas da empresa, incluindo matriz e filiais, colaboradores, parceiros externos e prestadores de serviços.

É exigido um termo de responsabilidade e ciência em que os usuários se comprometem a agir de acordo com a Política de Segurança da Informação. Para os colaboradores e parceiros externos, o termo é assinado no ato da contratação.

Para os contratos firmados com empresas terceiras, é exigida cláusula específica assegurando o compromisso com a confidencialidade das informações da Warren.

3. DIRETRIZES

Segurança da Informação: Processos e metodologias que são projetados, implementados, mantidos e atualizados para assegurar a confidencialidade, integridade e disponibilidade das informações através da tecnologia, pessoas e processos a fim de detectar, prevenir e responder às ameaças.

Usuários: Indivíduo, ou processo (sistema) agindo em nome de um indivíduo autorizado pelo proprietário do ativo da informação para os respectivos acessos.

Confidencialidade: É a propriedade da informação com o fim de assegurar que as informações não serão divulgadas a pessoas, processos ou tecnologias não autorizadas.

Disponibilidade: É a propriedade da informação com o fim de assegurar o acesso estável às informações sempre que necessário para usuários autorizados.

Integridade: É a propriedade da informação com o fim de assegurar que as informações não tenham sido alteradas acidental ou deliberadamente e que sejam precisas e completas.

Proprietário de Ativos de Informação: É o usuário com responsabilidade direta sobre determinados ativos de informação da Warren.

Dados Pessoais: Informação relacionada a pessoa natural identificada ou identificável.

Dados Pessoais Sensíveis: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

4. PAPÉIS E RESPONSABILIDADES

a) Área de Segurança da Informação

- Conduzir os esforços estratégicos para cumprimento dos objetivos de Segurança da Informação para toda a Warren;
- Estabelecer mecanismos de proteção com vistas a prevenir, detectar, reduzir, e mitigar as vulnerabilidades nos ativos de informação;
- Realizar ações com a finalidade de prevenir a ocorrência de incidentes de segurança;
- Orquestrar rotinas e procedimentos necessários para a resposta de incidentes;
- Realizar o monitoramento contínuo e detecção de ataques cibernéticos;
- Certificar o controle de acesso adequado dos usuários, impedindo acessos indevidos e/ou em demasia e liberando apenas os acessos devidamente autorizados;
- Garantir que os prestadores de serviços terceirizados e relevantes cumpram com nossas políticas e normas de segurança, bem como as obrigações regulamentares aplicáveis;
- Garantir a conscientização da equipe através de treinamentos mandatórios e avaliações periódicas;
- Revisar, anualmente, esta Política.

b) Usuários

- Comprometer-se a seguir as regras do Termo de Uso da Rede Corporativa, Computadores, Internet e E-mail;
- O usuário deve zelar pela segurança de suas credenciais de acesso (senha, múltiplo fator de autenticação, e chaves privadas) da rede corporativa, computadores, internet, e-mail corporativo e sistemas internos, não compartilhando com outras pessoas, utilizando senhas fortes e complexas, e habilitando o múltiplo fator de autenticação (MFA) sempre que suportado pelo sistema em questão;
- Ao se conectar em redes de computadores públicas (exemplo: aeroportos, cafeterias, entre outros) ou redes não corporativas, deve-se utilizar a solução de VPN homologada pela equipe de Infraestrutura de TI

e de Segurança da Informação com o objetivo de trafegar as informações de forma criptografada para evitar exposições indevidas do tráfego;
- Utilizar o e-mail corporativo apenas para fins estritamente profissionais, sendo proibida a comunicação pessoal e o envio de spam ou conteúdos não permitidos;
- Responder pela utilização inadequada de sistemas, internet, correio eletrônico, inclusive de outros usuários que estão sob sua gestão e/ou responsabilidade;
- Participar das campanhas de conscientização de segurança da informação.

c) Proprietários de Ativos de Informação

Salvo exceções, os gestores das áreas são os proprietários dos ativos de informação sob responsabilidade da sua área de atuação, e devem:

- Cumprir e transmitir as suas equipes as disposições estabelecidas pela Política e Normas de Segurança da Informação a fim de que o mesmo tenha ampla divulgação no ambiente de trabalho;
- Garantir que as inconformidades ocorridas em suas áreas sejam identificadas e reportadas, e que sejam adotadas as medidas corretivas apropriadas conforme controles de segurança da informação;
- Realizar os procedimentos adequados para desligamento e encerramentos contratuais vigentes;
- Proteger os ativos de sua área (físico e lógico), de acordo com os critérios de classificação das informações definidos pela Instituição;
- Aplicar sanções àqueles que deliberadamente violarem as determinações desta Política, suas Normas e Instruções, mediante orientação da área de Segurança da Informação;
- Avaliar as solicitações de acesso considerando a premissa de privilégio mínimo, que consiste em aprovar apenas os acessos essenciais com o fim de evitar permissões em demasia e desnecessárias.

d) Diretoria Executiva

- Divulgar e garantir que a presente Política seja cumprida integralmente;
- Aprovar, por unanimidade, a presente Política.

5. DIRETRIZES GERAIS

- A informação é um ativo que possui extremo valor e importância para a Warren e seus negócios;
- A alta direção da Warren está comprometida e apoia as metas e princípios de segurança da informação;

- As informações da Warren, dos seus clientes, e parceiros de negócios são tratadas e protegidas de forma ética e transparente, de acordo com as leis vigentes, regulações aplicáveis, e normas internas, apenas para a finalidade de negócio;
- Os acessos às informações e recursos serão concedidos apenas se houver a devida autorização da pessoa proprietária do ativo de informação em questão e do(a) líder da pessoa que solicitou o acesso;
- Para a concessão de acessos deve ser aplicado o conceito de privilégio mínimo, com acesso apenas aos recursos e informações imprescindíveis para a execução das atividades profissionais pertinentes à Warren;
- Cada usuário deve possuir uma identificação única (login de acesso), pessoal e intransferível, com garantia de rastreabilidade e não repúdio das ações executadas em recursos e informações da Warren, de seus clientes e parceiros de negócios;
- Qualquer informação ou produto resultante do trabalho dos usuários, no escopo de suas atividades contratadas, é de propriedade da Warren. Ao término do contrato de trabalho, os usuários devem manter as informações privadas e produtos gerados, salvo por cláusula contratual prevista, sob posse da Warren;
- A Warren se reserva o direito de monitorar, inspecionar ou auditar o acesso e o uso de aplicativos e informações de sua propriedade ou sob sua guarda com ou sem o consentimento, presença ou conhecimento dos usuários, mas respeitando aspectos legais;
- Nenhum software utilizado pela Warren para controle e proteção de suas informações pode ser alterado ou desabilitado pelos Usuários.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações da Warren devem ser classificadas em níveis, de acordo com a sua criticidade. Devem ser consideradas as necessidades de negócio e de compartilhamento ou restrição de acesso, com análise de impactos em relação ao uso indevido das informações. Os níveis de classificação da informação são:

Confidencial: Nível de classificação mais alto. São informações que podem comprometer as operações da organização, tanto em nível financeiro como em competitividade ou reputação e exige aprovação do(a) proprietário(a) do ativo de informação.

Restrita: Nível de confidencialidade médio. São informações estratégicas que devem ficar disponíveis apenas para determinados grupos de pessoas que obtiveram o acesso aprovado pelo(a) proprietário(a) do ativo da informação.

Interna: Nível de confidencialidade baixo. São informações que podem ser compartilhadas entre todos colaboradores e parceiros da Warren, mas não devem ser compartilhadas publicamente.

Pública: Nível de confidencialidade inexistente. São informações que não exigem sigilo e podem ser divulgadas para o público em geral, sem impacto ao negócio.

7. CONTRATAÇÃO DE SERVIÇOS DE TERCEIROS E DE COMPUTAÇÃO EM NUVEM

A contratação de serviços de terceiros para o processamento e armazenamento de dados, e de computação na nuvem deve seguir requisitos mínimos, avaliando a relevância do serviço contratado, criticidade, e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciados pelo serviço.

Conforme legislação aplicável, a contratação de novos serviços de processamento e/ou armazenamento de dados na nuvem deve ser comunicada ao BCB no prazo de até 10 dias após a contratação do serviço. A comunicação deve conter:

i. Nome da empresa contratada;
ii. Os serviços contratados;
iii. A indicação dos países e regiões onde os serviços poderão ser prestados e os dados poderão ser processados, armazenados e gerenciados.

O mesmo deve valer para alterações contratuais dos serviços contratados.

Os serviços contratados para processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que possam assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- A confidencialidade, integridade, e a disponibilidade das informações e dados armazenados e processados pelo prestador de serviços;
- O acesso aos dados e informações a serem processadas ou armazenados pelo prestador de serviço sempre que for necessário;
- Aderência as certificações exigidas pelo BCB;
- Acesso a relatórios de auditoria realizados por empresa especializada e independente, que ateste os procedimentos e os controles utilizados na prestação dos serviços a serem contratados;
- Disponibilidade de ferramentas e informações necessárias para realizar o monitoramento dos serviços prestados;
- Segregação dos dados dos clientes através de controles lógicos ou físicos;

- A disponibilização da quantidade e qualidade de controles de acesso implementados voltados à proteção dos dados da instituição;
- Adoção de controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos e sistemas disponibilizados pela internet.

Caso a operação do serviço contratado seja no exterior, deve ser verificada a existência de um convênio para troca de informações entre o BCB e as autoridades supervisoras dos países onde os serviços poderão ser prestados. No caso da inexistência de um convênio, deve ser solicitada a autorização para uso do serviço diretamente com o BCB com no mínimo 60 dias de antecedência.

Antes da assinatura do contrato com o prestador de serviços, deve ser definido quais são os países e as regiões dos países que podem ser utilizadas para o processamento e armazenamento das informações, certificando que todos os requisitos citados na legislação aplicável estão sendo cumpridos.

As informações contratuais e todos os documentos relativos ao contrato de prestação de serviços devem ficar à disposição do Banco Central do Brasil por cinco anos.

8. ESTRATÉGIA DE SEGURANÇA DA INFORMAÇÃO

A estratégia de Segurança da Informação da Warren é baseada em arquitetura com os seguintes domínios: Gestão de Segurança da Informação, Gestão de Identidades e Acessos, Segurança Cibernética Ofensiva, Segurança Cibernética Defensiva e Gestão de Continuidade de Negócios.

Para consolidação destes domínios, as políticas operacionais relacionados para nas seguintes áreas:

Classificação, manuseio e rotulagem da informação: A classificação das informações deve respeitar o ciclo de vida da informação desde a sua geração até o descarte. A rotulagem e o manuseio apropriado da informação e os seus ativos relacionados, no formato físico e eletrônico, deve ser realizado refletindo os níveis de classificação das informações conforme estabelecidos.

Cópias de segurança (Backup): Estabelece a política de backup, que define os requisitos da organização para as cópias de segurança das informações, dos softwares e dos sistemas. Deve ser mantido o registro completo e exato das cópias de segurança, provendo documentação apropriada sobre os procedimentos de restauração da informação.

Demandas e projetos: As demandas e projetos de negócio, serviços de retaguarda ou tecnologia devem estar em conformidade com as diretrizes, processos e arquitetura corporativa de segurança da informação. As demandas e projetos devem ser submetidos aos checklists de Segurança da Informação

aplicados pela área de Governança de TI, garantindo a sua aderência às melhores práticas e normativos de segurança.

Desenvolvimento Seguro de Aplicações e Sistemas: Os procedimentos para desenvolvimento de aplicações e sistemas devem seguir as boas práticas de mercado para a segurança, garantindo que a segurança da informação esteja projetada e implementada no ciclo de vida do desenvolvimento dos sistemas de informação.

Gestão de Ativos de Informação: Os ativos de informação devem ser identificados, inventariados e protegidos de acessos indevidos. Devem possuir documentação e rotinas de manutenção atualizadas.

Plano de Gestão de Continuidade de Negócios: Visa garantir que existam planos de continuidade de negócios e recuperação de desastres que contemplem alocação de profissionais, os principais processos e ativos de tecnologia e negócio da Warren.

Gestão de Identidade e Controle de Acesso: Às concessões, revogações, transferências e revisões de acesso devem respeitar os fluxos de aprovação e execução determinados pela Instituição, bem como se utilizar das ferramentas oficiais disponibilizadas para estes processos. Todos os acessos devem ser rastreáveis, possibilitando auditoria e responsabilidade individual de um usuário.

Gestão de Incidentes de Segurança da Informação: Os incidentes de segurança devem ser reportados à área de Segurança da Informação da Warren para o registro, a análise da causa e do impacto, e para o controle dos efeitos para as atividades da instituição. Após a identificação, contenção de danos, e investigação interna, deve ocorrer o compartilhamento de informações sobre incidentes relevantes conforme trata o art. 3º, inciso IV da Resolução 4.893/2021 ou Circular 3.909/2018.

É considerado incidente relevante qualquer incidente de segurança que afete processos críticos de negócios e comprometa a confidencialidade, integridade e disponibilidade das informações e de sistemas da Warren ou parceiros.

Será elaborado anualmente um relatório sobre a implementação do plano de ação e de resposta a incidentes, que deve ser apresentado a alta direção.

Política de Privacidade: Os procedimentos e controles relativos à coleta, processamento, proteção e compartilhamento de informações pessoais, respeitando os direitos de privacidade, à intimidade, honra, e outros direitos reservados ao titular dos dados, seguindo as leis e regulamentações de proteção de dados aplicáveis

Segurança Cibernética: Os procedimentos e os controles da segurança cibernética são implementados de modo a abranger a autenticação, criptografia, prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes de invasão e de outras metodologias de operações ofensivas para detecção e correção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de

rastreabilidade, os controles de acesso e de segmentação da rede de computadores, a manutenção de cópias de segurança dos dados e das informações, e a prevenção e reposta de incidentes de segurança da informação.

Segurança Física: Compreendem os procedimentos para proteger equipamentos e informações contra usuários que não possuem autorização para acessá-los. Para a execução deste processo, são solicitadas autorizações aos gestores responsáveis e conferidos os titulares, junto ao Departamento de Pessoas e Cultura, quando aplicável, inclusive para a concessão de acesso às dependências da Warren, segregando áreas com acesso restrito, por força de norma regulatória.

Treinamentos e Conscientização em Segurança da Informação: Visa o fortalecimento da cultura de Segurança da Informação através da disseminação dos princípios e diretrizes descritos nesta Política Geral de Segurança da Informação. Consiste no processo de capacitação e conscientização, de todos os níveis da Warren, ao que se refere à segurança da informação, contemplando segurança de dados, segurança cibernética, inclusive com relação aos terceiros e demais contrapartes.

Gestão de Riscos de Segurança da Informação: Os riscos de Segurança da Informação devem ser identificados e acompanhados através de um processo de análise de vulnerabilidades, quantificando e qualificando as ameaças e seus respectivos impactos sobre os ativos de informação, para associação dos níveis de proteção adequados.

9. REGULAMENTAÇÃO INTERNA RELACIONADA

- Código de Ética da Warren;
- Plano de Continuidade Operacional (PCO);
- Política de Privacidade da Warren;
- NP 04.001 - Norma de Segregação de Atividades;
- NP 04.002 - Norma de Gestão de Identidade e Controle de Acessos.

10. BASE REGULATÓRIA E LEGISLAÇÃO APLICÁVEL

- Resolução 4.557/2017 do Banco Central do Brasil;
- Resolução n° 4.893/2021 do Banco Central do Brasil;
- Lei Federal 12.965, de 23 de abril de 2014;
- Lei 13.709, de 14 de agosto de 2018.

11. REFERÊNCIAS NORMATIVAS

- Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos, Segunda Edição, ABNT NBR ISO/IEC 27001, 2013;
- Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação, Segunda Edição, ABNT NBR ISO/IEC 27002, 2013;
- Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem, ABNT NBR ISO/IEC 27017, 2016.

12. CONTROLE DE REVISÕES

Item	Data	Alteração	Revisado por
4.	30/07/2021	Inclusão de responsabilidades no uso de senhas, de internet, de correio eletrônico, de software e da Diretoria Executiva.	Jéssica Miranda

13. DISPOSIÇÕES FINAIS

Necessidades conflitantes com a PSI serão avaliadas pela equipe de Segurança da Informação.

Qualquer dúvida, sugestão e/ou solicitação que envolva esta Política de Segurança da Informação e de Privacidade de Dados, o colaborador deve entrar em contato com os seus gestores, equipe de Segurança da Informação, ou com Encarregado de Proteção de Dados da empresa.

Esta política deve ser revisada com a periodicidade mínima anual.