POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

09/2025

Classificação
Política

Título
Segurança da Informação e Cibernética

Versão
09

Data de atualização
30/09/2025

.

Sumário

1. OBJETIVO 3
2. APLICAÇÃO 4
3. BASE REGULATÓRIA 4
4. PRINCÍPIOS 5
5. DIRETRIZES GERAIS 5
5.1. CLASSIFICAÇÃO DA INFORMAÇÃO 6
5.2. Segregação Lógica e Controle de Administração de Acessos 7
5.3. Política de Senha 10
5.4. Descarte de Informações 12
5.5. Tratamento e Controle de Dados de Clientes 13
5.5.1. Monitoramento e Detecção de Roubo de Credenciais de Clientes 13
5.6. Prevenção contra vazamento de dados 13
5.7. Uso dos Recursos de Tecnologia da Informação 13
5.8. Serviços Relevantes de Terceiros 16
5.9. Criptografia – Proteção de Conteúdo 17
5.10. Prevenção e a Detecção de Intrusão 17
5.11. Gestão de Incidentes de Segurança 20
5.12. Backup e Recuperação de Dados 20
5.13. Gestão de Mudança 20
5.14. Monitoramento e Auditoria 21
5.15. Conscientização e Divulgação 21
5.16. Gerenciamento de Sessões – Gerenciamento de Sessões – Plataforma da Corretora 24
6. Exceção às Regras estabelecidas Neste Instrumento Normativo 24
7. Papéis e Responsabilidades 24
8. Documentos Vinculados 26
9. Vigência 26
10. Versionamento 27

1. OBJETIVO

Esta Política tem como objetivo estabelecer as regras e diretrizes relativas à Segurança da Informação e à Segurança Cibernética no âmbito do Grupo Warren (“Warren Rena” ou “Instituição”), visando proteger, de forma adequada e contínua, os ativos de informação, bem como os dados sensíveis de clientes, parceiros e colaboradores.

Busca-se, no mínimo, garantir a proteção contra ameaças internas, externas e riscos associados ao uso da informação, prevenindo acessos indevidos, modificações não autorizadas, vazamentos e interrupções.

2. APLICAÇÃO

As regras estabelecidas neste documento devem ser cumpridas pelos dirigentes, colaboradores, prestadores de serviços e parceiros externos vinculados ao Grupo Warren.

3. BASE REGULATÓRIA

- **Ofício Circular 132/2022-PRE, de 30 de setembro de 2022 132/2022-PRE:** Estabelece regras sobre o Programa de Qualificação Operacional (PQO) – Informações consolidadas do Manual de Certificação.

- **Resolução CVM nº 35, de 26 de maio de 2021:** Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e revoga a Deliberação CVM nº 105, de 22 de janeiro de 1991, e as Instruções CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, CVM nº 505, de 27 de setembro de 2011, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020.

- **Resolução BCB nº 85, de 08 de abril de 2021:** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.

- **Ofício-Circular CVM/SMI nº 5, de 04 de agosto de 2020**: Orientações sobre os prazos de comunicação à SMI referente às situações relacionadas ao PCN, Sistemas Críticos e Segurança Cibernética.

4. PRINCÍPIOS

O Grupo Warren adota padrões tecnológicos e operacionais de segurança da informação e segurança cibernética, com o objetivo de prevenir fraudes, invasões, vazamentos e acessos indevidos, assegurando o sigilo, a confiabilidade e a disponibilidade das informações e das comunicações internas e externas.

A Segurança da Informação e Cibérnetica da Instituição está fundamentada na preservação dos seguintes princípios fundamentais:

Confidencialidade: garante que as informações sejam acessadas somente por pessoas devidamente autorizadas e apenas durante o período necessário para o exercício de suas atividades.

Integridade e Autenticidade: assegura que as informações permaneçam completas, íntegras, consistentes e autênticas, não sendo alteradas, destruídas ou manipuladas de forma não autorizada ou acidental ao longo de seu ciclo de vida.

Disponibilidade: assegura que as informações estejam acessíveis e utilizáveis pelas pessoas autorizadas sempre que necessário, garantindo a continuidade dos processos de negócio e a tomada de decisão baseada em dados confiáveis.

Esses princípios norteiam todas as práticas, controles e decisões relacionadas à segurança da informação e cibernetica, afim de assegurar:

- A proteção dos dados de clientes, parceiros, colaboradores e da própria Instituição contra acessos indevidos, vazamentos e fraudes;
- Prevenir e detectar ameaças cibernéticas, internas e externas, que possam comprometer a integridade, confidencialidade ou disponibilidade das informações e sistemas corporativos;
- Garantir a continuidade das operações críticas, mesmo diante de incidentes, por meio de planos de resposta, recuperação e contingência;
- Estabelecer controles técnicos e organizacionais eficazes, como firewalls, sistemas de detecção e prevenção de intrusão, autenticação e gestão de vulnerabilidades;
- Promover a conscientização e a cultura de cibersegurança entre colaboradores, terceiros e demais públicos internos, com programas regulares de treinamento e simulações;
- Avaliar continuamente os riscos cibernéticos, adotando melhorias nos controles, processos e tecnologias de defesa.

5. DIRETRIZES GERAIS

As diretrizes a seguir estabelecem os principais controles, responsabilidades e boas práticas adotados pelo Grupo Warren para garantir a aplicação efetiva dos princípios de Segurança da Informação e Segurança Cibernética em seus processos, sistemas e relações com colaboradores, clientes, parceiros e terceiros.

Além disso, garantem que as regras e procedimentos implementados estejam compatíveis com:

(i) o porte, perfil de risco e modelo de negócio da Instituição,

(ii) a natureza das atividades e a complexidade dos produtos e serviços oferecidos, e

(iii) a sensibilidade dos dados e das informações sob responsabilidade da Instituição.

5.1. CLASSIFICAÇÃO DA INFORMAÇÃO

Com o objetivo de garantir a proteção adequada das informações sob responsabilidade do Grupo Warren, toda informação deve ser classificada de acordo com seu nível de sensibilidade, criticidade e impacto em caso de vazamento, modificação ou indisponibilidade.

Na ausência de classificação formal, toda informação deve ser considerada, no mínimo, como Interna.

5.1.1. Categorias De Classificação

A Instituição adota as seguintes categorias de classificação:

Confidencial Informações estratégicas, comerciais, financeiras ou técnicas, cujo vazamento pode causar prejuízos significativos à Instituição ou a terceiros.

Exemplos: dados de clientes, contratos, planos de negócios, códigos-fonte, senhas, registros de auditoria e dados pessoais sensíveis.

O tratamento inadequado dessas informações pode resultar em multas, sanções regulatórias, perda de clientes, impactos à reputação e vantagem competitiva a terceiros.

Restrita: Informações com nível intermediário de sensibilidade, cujo acesso deve ser limitado a grupos específicos previamente autorizados pelo(a) proprietário(a) do ativo da informação.

Exemplos de informações restritas: relatórios com dados pessoais ou financeiros, relatórios financeiros em elaboração, planos de desenvolvimento individual

Interna: Informações de uso restrito aos colaboradores e prestadores autorizados, cujo acesso indevido pode gerar impactos operacionais ou de imagem.

Exemplos: manuais internos, relatórios operacionais, procedimentos administrativos.

Pública: Informações que podem ser divulgadas ao público sem restrições, como conteúdos institucionais em sites, materiais de marketing e comunicados oficiais.

5.1.2. Dados Sensíveis

O Grupo Warren observa e cumpre rigorosamente toda a legislação aplicável à segurança da informação, privacidade e proteção de dados pessoais, incluindo — sempre que pertinentes — a Constituição Federal, o Código de Defesa do Consumidor, o Código Civil, o Marco Civil da Internet (Lei nº 12.965/2014 e Decreto nº 8.771/2016), a Lei

Complementar nº 105/2001 (Sigilo Bancário), a Lei Complementar nº 166/2019, a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), a Lei nº 13.853/2019, além de demais normas regulatórias aplicáveis.

De acordo com a LGPD:

- **Dados Pessoais** são informações relacionadas a pessoa natural identificada ou identificável;
- **Dados Sensíveis** são dados pessoais que revelem origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

Portanto, em conformidade com as exigências regulatórias, o Grupo Warren considera como dados sensíveis todos os dados cadastrais e demais informações que permitem a identificação de clientes, suas operações e posições de custódia.

Essa classificação reforça o compromisso da Instituição com a proteção, o controle de acesso e a governança adequada dessas informações, aplicando medidas técnicas e administrativas compatíveis com seu nível de criticidade.

5.1.3. Critérios para Classificação

Em caso de dúvidas quanto à classificação de determinada informação, recomenda-se considerar as seguintes perguntas orientadoras:

- Esta informação pode ser compartilhada com o público externo sem prejuízo? → Pública
- Pode ser acessada por todos os colaboradores da empresa? → Interna
- Deve ser acessada apenas por grupos restritos e aprovados? → Restrita
- Deve ser acessada somente por sócios ou pessoas específicas e autorizadas? → Confidencial

5.2. Segregação Lógica e Controle de Administração de Acessos

5.2.1. Controle de Acessos

A Instituição adota controles formais e estruturados para a gestão de acessos aos sistemas, bases de dados e recursos corporativos, com foco na segregação de funções e na mitigação de riscos operacionais.

Esses controles têm como objetivo prevenir conflitos de interesse, uso indevido de informações e acessos indevidos, assegurando que as permissões sejam concedidas de acordo com os princípios do menor privilégio e da necessidade de acesso, com base nas atribuições e responsabilidades de cada função.

As diretrizes de controle de acesso são aplicáveis a todos os usuários da Instituição, em todos os níveis hierárquicos e áreas de atuação.

O processo de concessão, manutenção e revogação de acessos deve observar, no mínimo, os seguintes requisitos:

a) O acesso deve ser individual, exclusivo e intransferível, sendo vedado o compartilhamento de credenciais;
b) Quando aplicável, o usuário deve possuir as certificações ou habilitações exigidas para a função;
c) A concessão de acesso deve ser aprovada formalmente pelo(a) proprietário(a) da informação;
d) O acesso deve ser concedido somente a profissionais vinculados à Instituição, incluindo colaboradores, prepostos e terceiros contratados;
e) Os acessos devem ser compatíveis com a função desempenhada, de forma a evitar conflitos de interesse e excessos de privilégio.

A Warren Rena mantém procedimento específico, integrante desta Política, que disciplina de forma detalhada os fluxos de solicitação, aprovação, concessão, revisão periódica e revogação de acessos, com base em controles de trilhas de auditoria e revisões regulares de permissões.

5.2.2. Segregação de Funções

A Segregação de Funções é um dos pilares essenciais de controle interno adotado pela Warren Rena. Consiste na distribuição adequada de responsabilidades entre diferentes profissionais, de modo a evitar a concentração de atribuições que possam gerar riscos operacionais, conflitos de interesse ou fragilidades nos processos de controle.

Nenhum colaborador deve, sob qualquer hipótese, deter poderes, acessos ou atribuições que conflitem entre si, em desacordo com as práticas de segregação estabelecidas.

Para esse fim, a Warren Rena mantém uma Matriz de Segregação de Funções (“Matriz”), que define:

- Define as atividades críticas executadas nos sistemas utilizados pela Instituição;
- Identifica os potenciais conflitos de interesse decorrentes da execução simultânea de determinadas funções por um mesmo profissional;
- Especifica os proprietários das informações de cada sistema ou processo;
- Estabelece, quando aplicável, os requisitos de certificação ou habilitação necessários ao uso dos sistemas.

A Matriz deve ser consultada previamente à concessão de acessos, e suas diretrizes devem ser aplicadas de forma rigorosa.

Entre os conflitos mínimos de atividades a serem evitados, destacam-se:

i. Transferência de custódia de clientes realizada por profissionais que também desempenham atividades operacionais;
ii. Inclusão ou alteração de limites pré-operacionais de clientes por profissionais que atuam em operações;
iii. Atualização de dados bancários de clientes por profissionais vinculados à área de liquidação.

A Warren Rena possui procedimento específico que complementa esta Política, detalhando os critérios, responsabilidades, fluxos e mecanismos de controle relativos à

segregação de funções e prevenção de conflitos de interesse nos ambientes sistêmicos e operacionais.

5.2.3. Usuário não Nominal Genérico

Usuário genérico é toda credencial de acesso criada sem vinculação direta e individualizada a um único colaborador, , ou seja, não associada a um nome pessoal.

Através do Termo de Responsabilidade – Usuário Genérico não Nominal - Colaboradores, o usuário responsável pelo usuário não nominal ficará ciente das atribuições de suas responsabilidade, guarda de informações, penalidades, sigilo, confidencialidade e obrigações pertinentes à privacidade e à Lei Geral de Proteção de Dados – LGPD (lei 13.709/2018.

A área de Segurança da Informação é responsável por realizar, anualmente, a revisão formal de todos os usuários genéricos existentes na Instituição, com o objetivo de garantir a efetividade dos controles de acesso.

Caso sejam identificadas inconsistências ou desconformidades, estas deverão ser analisadas quanto às suas causas e tratadas com ações corretivas apropriadas.

5.2.4. Segurança Física

Segurança física é o conjunto de medidas adotadas para proteger fisicamente os ativos de informação da Instituição contra acessos não autorizados, danos, furtos, perdas ou interferências externas.

A Warren Rena adota as seguitentes diretrizes para assegurar a proteção do seus ativos

Pessoas Autorizadas

O acesso físico às dependências da Instituição, é restrito a pessoas previamente autorizadas.

As autorizações devem ser concedidas com base no princípio da necessidade de acesso, respeitando os critérios de função e nível de responsabilidade. O acesso deve ser revogado imediatamente em caso de mudança de função, desligamento ou fim do contrato.

Todos os acessos devem ser registrados em sistema ou controle físico apropriado e mantidos para fins de monitoramento, rastreabilidade e auditoria, por período mínimo de 5 (cinco) anos.

Áreas Seguras

São consideradas áreas de segurança todos os locais que abrigam servidores de aplicação, bancos de dados, equipamentos de rede (como firewalls), unidades de backup e a Mesa de Operações.

É terminantemente proibida a presença de clientes no ambiente da Mesa de Operações, sob qualquer circunstância.
Terceiros que necessitem acessar a Sala dos Servidores devem seguir todas as normas de segurança descritas nesta Política e ser acompanhados por profissional qualificado e autorizado durante todo o período de permanência.

Credenciais de Acesso
Todos os colaboradores devem possuir credencial individual para acesso à entrada principal do prédio e aos elevadores.
O acesso de prestadores de serviços de TI e terceiros (contratados ou não) deve ser monitorado e controlado.
A credencial é pessoal e intransferível — seu uso por terceiros não autorizados é proibido.
A responsabilidade pela guarda e conservação da credencial é do próprio prestador ou terceiro.
Em caso de perda ou extravio, a área responsável pela contratação deve ser imediatamente comunicada para o bloqueio e adoção das providências cabíveis.

Sistemas de Segurança Inteligente

A Instituição utiliza sistemas de segurança inteligente, como reconhecimento facial e biometria, para controle de acesso às dependências. Tais sistemas permitem restringir o ingresso de pessoas não autorizadas e reforçam a segurança física e lógica dos ambientes críticos.

5.2.5. Gerenciamento do Ciclo de Vida dos Usuários Desligados

A Instituição estabelece controles para garantir a revogação oportuna de acessos de colaboradores, terceiros, estagiários e prestadores de serviços desligados, evitando o risco de uso indevido de credenciais inativas.

O processo de desligamento deve contemplar, no mínimo:

- Comunicação imediata entre as áreas responsáveis (Gente e Gestão, Segurança da Informação e Tecnologia) sobre o desligamento do usuário;
- Revogação de acessos a todos os sistemas, aplicações, redes e recursos físicos e lógicos vinculados ao usuário desligado;
- Bloqueio ou exclusão de contas de e-mail, ferramentas colaborativas e dispositivos móveis corporativos vinculados ao colaborador;
- Devolução e inventário de equipamentos e ativos sob a responsabilidade do usuário desligado, como notebooks, tokens, celulares, entre outros;

5.3. Política de Senha
5.3.1. Configurações de Senhas

Os Colaboradores são responsáveis pela confidencialidade de suas respectivas senhas, que são individuais e intransferíveis.

Devem ser seguidas as regras determinadas pela Gerência de Segurança da Informação, no momento da configuração e do cadastramento de senha.

5.3.2. Parâmetros de Senhas e de Segurança: Sistemas Internos Críticos

Os parâmetros utilizados devem observar, minimamente, os seguintes critérios:

Parâmetros avaliados	Descrição
Autenticação forte	Critérios de composição de senha com o objetivo de garantir que o usuário defina uma senha forte para dificultar a descoberta por tentativas de adivinhação de senhas.
Adivinhação da senha	Bloqueio da conta e/ou notificação ao administrador sobre tentativas de acesso com uma senha incorreta, após determinado número de tentativas de acesso inválidas.
Reutilização de senha	Mecanismos que proíbem a reutilização das últimas senhas definidas pelo usuário.
Desbloqueio da senha	Procedimentos de desbloqueio de senha pelo administrador mediante a confirmação da identidade do usuário.
Armazenamento criptografado	Armazenamento da senha nos bancos de dados de forma criptografada, utilizando algoritmos de ao menos 128 bits.
Troca de senha padrão	Obrigatoriedade da troca de senha padrão ou de conhecimento do mercado no primeiro acesso do usuário.

5.3.3. Requisitos mínimos de Senhas e de Segurança

Considerando as características do negócio da Warren Rena e melhores práticas de mercado, os sistemas utilizados por usuários internos e externos (clientes), deverão possuir, minimamente, os seguintes critérios:

Requisitos avaliados	Requisitos mínimos (RB 124)	Tipo de Acesso (A)	Descrição dos requisitos
Tamanho mínimo da senha	6 caracteres	Client e Canal de Relacionamento (Site e Mobile)	A senha deverá ser composta por no mínimo 6 caracteres.
Desbloqueio mediante confirmação de identidade	Ativado	Client e Canal de Relacionamento (Site e Mobile)	O desbloqueio da senha não poderá ser realizado sem a confirmação de dados cadastrais do cliente.
Criptografia da senha	Ativada	Client e Canal de Relacionamento (Site e Mobile)	O armazenamento da senha deverá ser realizado de forma criptografada, utilizando algoritmo de ao menos 128 bits.
Troca de senha no primeiro acesso	Ativada	Client e Canal de Relacionamento (Site e Mobile)	A senha deverá ser trocada no primeiro acesso, quando não for definida pelo próprio cliente.
Segundo fator de autenticação	Ativado	Canal de Relacionamento (Site e Mobile)	O acesso eletrônico utilizado para transações deverá possuir Segundo Fator de Autenticação, que deve ser distinto da senha utilizada na primeira autenticação do usuário.
Certificado digital	Ativado	Canal de Relacionamento (Site)	O site (canal de relacionamento) deverá possuir certificado digital emitido por autoridade certificadora aprovada pela ICP Brasil ou equivalente.

Criptografia no tráfego das informações	Ativado	Canal de Relacionamento (Site)	O tráfego de consulta e edição de informações pessoais deverá ser criptografado com algoritmo de, no mínimo, 256 bits ou por método que proporcione segurança equivalente.

(A) Descrição do tipo de acesso: (i) client: sistemas eletrônicos de negociação fornecidos e gerenciados pelo Participante ou por terceiros por ele contratado que são acessados por meio de aplicações instaladas nas estações de trabalho dos clientes; (ii) Canal de Relacionamento – Site: canais de relacionamento eletrônico, disponibilizados pelo Participante para consulta e transações, que são acessados por clientes por meio de browser de navegação (site); e (iii) Canal de Relacionamento – Mobile: canais de relacionamento eletrônico, disponibilizados pelo Participante para consulta e transações, que são acessados por clientes por meio de aplicativos instalados em dispositivos móveis (os parâmetros serão avaliados separadamente por plataformas - Android e iOS).

5.3.4. Exceções Parâmetros de Senha

Em casos de sistemas com limitações técnicas, a Instituição adapta sua política de segurança de senhas para adotar os parâmetros mais seguros possíveis, respeitando as restrições da aplicação.

Qualquer exceção às regras de senha descritas nesta Política deverá ser avaliada previamente pela Área de Segurança da Informação e, quando necessário, formalizada por meio do fluxo de exceção à política, com a devida justificativa técnica e aprovação documentada.

5.4. Descarte de Informações

Todos os colaboradores devem zelar pela proteção das informações sob sua responsabilidade, especialmente aquelas que possam representar vantagens competitivas ou gerar impactos financeiros, jurídicos ou à imagem da Instituição.

O descarte de documentos e mídias que contenham informações sensíveis deve ocorrer de forma segura, somente ao final do ciclo de vida da informação, considerando os prazos legais e regulatórios de retenção aplicáveis.

Documentos físicos com informações sensíveis devem ser descartados com segurança, incluindo, mas não se limitando a:

- Contratos de qualquer natureza;
- Relatórios com classificação restrita ou confidencial;
- Documentos com dados de clientes (ex: extratos, propostas, formulários).

O descarte de mídias físicas deve seguir os seguintes procedimentos:

- Cartões bancários ou de crédito: devem ser cortados em pequenos pedaços, assegurando que a área magnética seja inutilizada;
- CDs, DVDs e pendrives: devem ser quebrados ou destruídos fisicamente de modo a impedir a recuperação de dados;
- Discos rígidos (HDs): devem ser formatados fisicamente e destruídos, impedindo sua reutilização ou acesso futuro às informações ali armazenadas.

5.5. Tratamento e Controle de Dados de Clientes

O Grupo Warren adota medidas técnicas, administrativas e organizacionais para assegurar o tratamento adequado, ético e seguro dos dados de seus clientes, em conformidade com a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), bem como com as normas e exigências regulatórias.

Além desta Política de Segurança da Informação, o tema é disciplinado por política específica.

5.5.1. Monitoramento e Detecção de Roubo de Credenciais de Clientes

A Warren Rena mantém um Security Operations Center (SOC) em operação ininterrupta, 24 horas por dia, 7 dias por semana, responsável pelo monitoramento contínuo da segurança da rede e de diversas fontes de eventos relacionados à segurança da informação.

O SOC conta com uma equipe especializada em inteligência de ameaças (Threat Intelligence), que realiza investigações proativas na deep web e dark web com foco na identificação antecipada de sinais de roubo, vazamento ou exposição de credenciais de clientes.

Sempre que uma ameaça potencial é detectada, a equipe do SOC atua prontamente na contenção e mitigação do risco, adotando medidas técnicas e administrativas para proteger os dados dos clientes e preservar a integridade dos sistemas.

Esse modelo de monitoramento contínuo aliado à resposta rápida é um dos pilares da estratégia de segurança da Instituição, reforçando os princípios de confidencialidade, integridade e disponibilidade das informações sob sua guarda.

5.6. Prevenção contra vazamento de dados

Como parte de sua estratégia de proteção da informação, a Warren Rena adota controles preventivos, técnicos e administrativos para reduzir o risco de vazamento de dados em seus ambientes internos e externos.

As diretrizes detalhadas sobre os mecanismos de prevenção estão formalizadas no documento específico.

5.7. Uso dos Recursos de Tecnologia da Informação

Todos os colaboradores que tenham acesso aos ativos de informação e recursos de tecnologia da informação da Instituição são responsáveis por zelar pela sua integridade, confidencialidade, disponibilidade e uso adequado.

Esses recursos devem ser utilizados de forma ética, segura e exclusivamente para fins profissionais, respeitando as políticas internas, a legislação vigente e as regulamentações aplicáveis.

Uso de E-mail

O uso do e-mail corporativo deve ser realizado exclusivamente para fins institucionais, sendo vedado seu uso como meio de comunicação pessoal ou particular.

Toda informação transmitida por e-mail deve ser tratada como propriedade da Instituição, e deve refletir a conduta profissional esperada.

Com o objetivo de preservar a segurança da informação e garantir a conformidade com esta Política, a Instituição reserva-se o direito de monitorar, registrar e auditar o conteúdo de todas as mensagens enviadas ou recebidas por meio do e-mail corporativo.

Uso das Redes Sociais

Comentários relacionados aos processos e as atividades executadas na Instituição, não devem ser realizados (por áudio, texto ou vídeos) nos meios de comunicação social, mesmo que já tenham se tornado público por meio da mídia.

Os colaboradores devem assegurar a confidencialidade e a integridade das informações pertencentes à Instituição.

Ramais com Gravação de Ligações

Colaboradores de áreas sujeitas a exigência regulatória de gravação devem estar cientes de que todas as ligações realizadas por meio dos ramais designados são gravadas. As gravações devem ser arquivadas em formato digital, com prazo mínimo de retenção de 5 (cinco) anos.

O processo para acesso as gravações seguem os procedimentos definidos no item 5.3. deste documento.

Uso da *Internet*

A Instituição disponibiliza acesso à internet aos seus colaboradores com o objetivo de apoiar o desempenho de suas atividades profissionais, fornecendo acesso a recursos e informações complementares, quando necessário.

Contudo, o uso da internet deve seguir rigorosamente os critérios de segurança, conformidade e responsabilidade definidos por esta Política, sendo expressamente vedada a execução ou o download de ferramentas não homologadas.

Caso haja necessidade de realizar downloads específicos ou acessar endereços bloqueados por ferramentas de controle, deve ser seguido os procedimentos definidos no item 5.3. deste documento.

A Instituição não aprova, em hipótese alguma, o uso indevido ou de maneira ofensiva da internet, ficando os colaboradores, prestadores de serviços de TI ou terceiros contratados de TI sujeitos à advertência e/ou às penalidades administrativas cabíveis.

Não são permitidos, em hipótese alguma, a divulgação e/ou o compartilhamento indevido de informações relacionadas à Instituição em sites, comunidades de relacionamento, salas

de bate-papo, chat ou qualquer outra forma de comunicação que venha a ser desenvolvida e utilizada por meio da Internet.

Instalação de *Softwares* ou Aplicativos

A instalação de softwares nos ambientes da Instituição é restrita a aplicações previamente homologadas e aprovadas pelas áreas responsáveis. Apenas *softwares* que tenham passado pelos processos de validação técnica e de segurança podem ser instalados.

Caso haja necessidade de utilização de um *software* ainda não homologado, o solicitante deverá abrir uma demanda formal para análise e aprovação.

Além disso, mecanismos de controle estão implementados para prevenir o download e a instalação de softwares não autorizados.

Esse procedimento tem como objetivo preservar a integridade, a segurança e a conformidade do ambiente tecnológico da Instituição.

Redes *Wireless*

Para garantir a segurança e a eficiência de nossas redes sem fio, a Warren Rena destinou redes *wireless* para ao uso de dispositivos pessoais de nossos colaboradores e visitantes e redes corporativas projetadas exclusivamente para uso nos computadores corporativos, permitindo o acesso aos recursos internos da rede corporativa.

Tal distintação busca evitar a sobrecarregar nossos links de internet e priorizar o acesso aos recursos internos da empresa.

Para garantir a segurança dessa rede, é obrigatória a instalação do certificado digital para autenticação EAP-TLS mútua entre o cliente (computador corporativo) e o servidor da rede. Essa autenticação adicional ajuda a prevenir acessos não autorizados e proteger nossos recursos internos contra ameaças.

Ao utilizarem as redes corporativas, nossos colaboradores têm acesso direto aos recursos internos da rede corporativa, facilitando a colaboração e o trabalho em equipe. Importante destacar que as redes corporativas não possuem limitação no uso da largura de banda. Isso significa que os computadores corporativos têm uma conexão mais robusta e rápida para acessar os recursos necessários.

É fundamental que todos os colaboradores compreendam a importância de utilizar as redes *wireless* corretamente. Lembramos a todos que o uso adequado das redes *wireless* é essencial para manter a segurança de nossos sistemas e informações confidenciais. Portanto, é responsabilidade de cada colaborador seguir as diretrizes e políticas estabelecidas para o uso das redes wireless em nossos escritórios.

Utilização de Notebooks e/ou Desktop

O colaborador custodiante do notebook e/ou do computador móvel deve se responsabilizar pela integridade e pela segurança do equipamento.

O notebook e/ou Desktops devem ser utilizados de acordo com as regras de segurança descritas nesta Política, é importante ressaltar que, as informações existentes nestes recursos devem ser consideradas propriedade da Instituição.

O colaborador custodiante não deve em nenhuma hipótese instalar qualquer tipo de software ou hardware no equipamento sem o devido conhecimento da Área de Infraestrutura e Segurança, a qual deve homologar o respectivo aplicativo e aprovar sua instalação.

Os equipamentos devem ser configurados pela área de Infraestrutura e/ou parceiro fornecedor das máquinas, visando a garantia da segurança, entre eles, antivírus, tokens de autenticação, criptografia.

Segurança do Hardware em Ambiente de Rede

Para assegurar a continuidade operacional e a integridade dos ativos físicos de tecnologia, os equipamentos de rede e servidores devem ser instalados e mantidos de acordo com boas práticas de infraestrutura e segurança física:

- Os equipamentos devem estar conectados a rede elétrica estabilizada, com aterramento adequado e proteção contra picos de energia;
- Devem ser instalados em ambientes apropriados, protegidos de exposição solar direta, calor excessivo e acúmulo de poeira;
- O uso de nobreaks devidamente dimensionados é obrigatório, garantindo:
- Estabilização da tensão elétrica;
- Tempo hábil para salvamento de dados e desligamento seguro em caso de falha de energia;
- Os servidores devem estar alocados em sala exclusiva e restrita, com acesso controlado conforme definido na Matriz de Segregação de Acessos;
- O sistema de prevenção de incêndio deve ser mantido em conformidade com as especificações do fabricante, com manutenções periódicas devidamente evidenciadas, como por meio de etiquetas nos extintores.

Essas medidas visam preservar a segurança dos equipamentos e a disponibilidade dos serviços críticos da Instituição.

5.8. Serviços Relevantes de Terceiros

Nos casos de contratação de terceiros para execução de serviços relevantes, os contratos firmados pela Instituição devem conter cláusulas específicas que garantam a proteção adequada das informações e a conformidade com os normativos aplicáveis.

Esses contratos devem assegurar, no mínimo:

- O cumprimento das exigências de manutenção de informações previstas no art. 48, inciso II, da Resolução CVM nº 35;

- A observância dos princípios de segurança da informação, especialmente a confidencialidade, integridade e disponibilidade dos dados tratados;
- A aderência aos requisitos da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018);
- A formalização de um Acordo de Nível de Serviço (SLA) que defina prazos, responsabilidades e padrões de qualidade;
- Regras claras sobre backup, armazenamento seguro e recuperação de dados, inclusive em ambientes externos ou nuvem, quando aplicável.

A Instituição possui um procedimento específico que regulamenta a contratação e gestão de terceiros prestadores de serviços relevantes.

5.9. Criptografia – Proteção de Conteúdo

Com o objetivo de assegurar a confidencialidade, integridade e autenticidade das informações trafegadas e armazenadas, a Warren Rena adota práticas robustas de criptografia, tanto em trânsito quanto em repouso.

5.9.1. Criptografia em Trânsito

A Warren Rena adota controles de criptografia como medida essencial para a proteção das informações sensíveis e confidenciais sob sua responsabilidade. A criptografia é utilizada tanto para proteger dados em trânsito — durante sua transmissão por redes internas ou externas — quanto para proteger dados em repouso, armazenados em sistemas e repositórios da Instituição.

São aplicadas práticas que envolvem o uso de protocolos atualizados, chaves criptográficas seguras e mecanismos que garantem a confidencialidade, integridade e autenticidade das informações. O gerenciamento desses controles considera critérios técnicos, regulatórios e de risco, assegurando que o acesso e o uso das informações ocorram de forma segura e controlada.

Essas medidas contribuem para mitigar riscos de vazamento, interceptação ou uso indevido de dados, preservando os interesses da Instituição, de seus clientes e demais partes envolvidas.

5.10. Prevenção e a Detecção de Intrusão

A Warren Rena adota práticas avançadas de segurança cibernética com foco na prevenção e detecção de intrusões, visando proteger seus sistemas, redes e ativos de informação contra acessos indevidos, ataques maliciosos e ameaças cibernéticas.

As medidas adotadas incluem a implementação de soluções especializadas de segurança que monitoram continuamente os sistemas, redes e aplicações da Instituição, com capacidade de detecção de comportamentos anômalos, análise de tráfego, identificação de vulnerabilidades e alertas em tempo real para equipes responsáveis pela segurança.

A Instituição mantém ainda processos automatizados e integrados que permitem respostas rápidas a incidentes, incluindo bloqueio de conexões suspeitas, contenção de ameaças, investigação de causa raiz e aplicação de medidas corretivas e preventivas.

Esses mecanismos abrangem tanto os ambientes locais, quanto os ambientes em nuvem, com cobertura sobre dispositivos, servidores, redes, aplicações web e dados armazenados.

Adicionalmente, são realizados periodicamente testes de segurança, como varreduras de vulnerabilidades, simulações de ataques (testes de intrusão) e avaliações de conformidade com boas práticas e normativos regulatórios, reforçando o compromisso com a melhoria contínua da postura de segurança cibernética da Instituição.

5.10.1. Monitoramento Contínuo e Detecção de Ataques Cibernéticos

A Área de Segurança da Informação é responsável por realizar o monitoramento contínuo dos ambientes tecnológicos da Instituição, utilizando ferramentas e processos voltados à identificação de atividades suspeitas e à detecção de ataques cibernéticos.

O Programa de Segurança Cibernética instituído deve ser revisado ao menos anualmente, ou sempre que alterações relevantes nos riscos, tecnologias ou operações assim exigirem. Além disso, o programa deve ser testado periodicamente, por meio de:

- Avaliação contínua de vulnerabilidades e exposição a ataques cibernéticos;
- Identificação de novos vetores de risco e ameaças emergentes;
- Verificação da eficácia das regras, controles e procedimentos existentes;
- Proposição de aprimoramentos com base nos resultados obtidos nas análises e testes realizados.

5.10.2. Proteção contra softwares maliciosos

A proteção contra códigos maliciosos é uma medida fundamental para assegurar a integridade dos sistemas e a disponibilidade da rede interna da Instituição. Por isso, todos os equipamentos de informática patrimoniados e conectados à rede corporativa — como computadores e *notebooks* — devem possuir *software* antivírus corporativo instalado, configurado e permanentemente atualizado.

Caso seja constatada a ausência do antivírus ou sua desatualização, a máquina deve ser imediatamente bloqueada para acesso à rede até que a situação seja regularizada, conforme determinação da Gerência de Segurança da Informação.

Cabe à Gerência de Segurança da Informação realizar o controle e a revisão periódica do ambiente, assegurando que todos os equipamentos estejam devidamente protegidos, de modo a preservar um ambiente tecnológico seguro e confiável para os colaboradores.

5.10.3. Controle de Vírus e Códigos Maliciosos

As estações de trabalho, *notebooks* e servidores utilizados na Instituição devem estar protegidos por soluções de segurança que realizem a detecção, controle e remoção de vírus e outros códigos maliciosos. A proteção deve operar em tempo real, com atualizações automáticas e sem a possibilidade de desativação por parte do colaborador.

Esse mesmo padrão de proteção deve ser aplicado aos e-mails enviados pela Instituição, de forma a prevenir o envio ou recebimento de mensagens com conteúdo malicioso, anexos suspeitos ou *links* perigosos.

Além disso, toda comunicação entre a rede interna da Instituição e redes externas deve ser monitorada por ferramentas de segurança que possibilitem a detecção de tentativas de intrusão, a aplicação de controles apropriados, o registro de eventos e a geração de evidências para fins de auditoria e resposta a incidentes.

5.10.4. Firewall de Aplicação - Proxy de Serviços

O firewall de aplicação, também conhecido como *proxy* de serviços, é utilizado como uma solução de segurança que atua como intermediário entre os dispositivos da Instituição e a rede externa (Internet), impedindo a comunicação direta entre origem e destino. Essa arquitetura contribui para a proteção contra acessos indevidos e ataques externos.

Caso haja qualquer suspeita de violação de segurança relacionada ao uso do *proxy*, a Área de Segurança da Informação deve ser imediatamente comunicada. A ocorrência deve ser formalmente registrada, com descrição das ações adotadas, histórico do evento e evidências correspondentes, de modo a permitir controle e rastreabilidade do incidente.

A senha de acesso ao firewall de aplicação deve ser tratada com absoluto sigilo e não pode, em hipótese alguma, ser compartilhada com terceiros. Caso seja necessário conceder acesso temporário a prestadores de serviço para fins de manutenção, a senha deverá ser alterada imediatamente após a conclusão do serviço.

A inclusão das regras de firewall é realizada pela Área de Infraestrutura seguindo o fluxo de aprovação das áreas responsáveis e periodicamente é realizada a revisão das regras criadas no firewall.

5.10.4.1. Revisão e Alteração das Regras de Firewall

As regras de firewall da Instituição devem ser revisadas periodicamente.

Toda e qualquer alteração nas regras de firewall deve ser formalizada por meio de um processo de Gestão de Mudanças (GMUD), contendo a descrição técnica detalhada da modificação proposta. A execução da mudança somente será permitida após a devida aprovação formal das áreas responsáveis.

As alterações devem ser integralmente documentadas, com registro das evidências de aprovação, data de implementação, responsáveis técnicos e justificativa da mudança. Esse controle visa garantir a rastreabilidade e a transparência do processo, além de mitigar riscos relacionados a configurações inadequadas ou não autorizadas.

5.10.5. Atualização de Segurança de Sistema Operacional

A Instituição reconhece a importância da atualização contínua dos sistemas operacionais como medida fundamental para garantir a segurança, o desempenho e a estabilidade de seus ativos tecnológicos.

Todos os computadores e *notebooks* internos devem ser submetidos, de forma periódica, às atualizações de segurança recomendadas pelos fornecedores, a fim de corrigir vulnerabilidades conhecidas, aprimorar funcionalidades e mitigar riscos cibernéticos.

5.11. Gestão de Incidentes de Segurança

A Warren Rena adota medidas preventivas e reativas para identificar, registrar, tratar e comunicar incidentes de segurança da informação, incluindo aqueles de natureza cibernética, que possam comprometer a confidencialidade, integridade ou disponibilidade dos dados e sistemas da Instituição.

Em caso de incidentes de segurança que afetem clientes, a organização realizará a comunicação de forma clara e adequada, conforme exigência regulatória.

As diretrizes, responsabilidades e fluxos operacionais para resposta a incidentes estão detalhados em procedimento específico que compõe esta Política, o qual estabelece os padrões a serem seguidos pela equipe técnica e pelas áreas envolvidas, conforme a natureza e criticidade do incidente.

5.12. Backup e Recuperação de Dados

A Warren Rena adota práticas e procedimentos para garantir a realização periódica de backups das informações críticas, visando assegurar a disponibilidade e a recuperação de dados em caso de falhas, incidentes ou desastres.

As diretrizes, responsabilidades, periodicidade, formas de armazenamento e testes de restauração estão detalhadas em documento específico.

5.13. Gestão de Mudança

A Warren Rena adota controles para assegurar que todas as alterações em sistemas, aplicações, infraestrutura e ambientes tecnológicos sejam planejadas, avaliadas, aprovadas e registradas formalmente, a fim de minimizar riscos à segurança da informação, à continuidade operacional e à conformidade regulatória.

As diretrizes e procedimentos relacionados à gestão de mudanças estão detalhados em documento específico.

5.14. Monitoramento e Auditoria

Tendo em vista a sua importância estratégica para o bom funcionamento das operações e dos negócios, os sistemas utilizados pela Instituição mantêm dados e registros organizados de forma estruturada, possibilitando a rastreabilidade completa das ações realizadas. Esses sistemas são capazes de identificar a origem de cada registro, alerta ou ocorrência, permitindo o monitoramento preciso e a análise de eventos por área,

5.14.1. Proteção e Revisão de Registro de Eventos (Logs)

Os sistemas utilitários como gerenciador de banco de dados e outras ferramentas de gestão de rede, especialmente as que acessam dados em Produção, geram o Registro de Operações, é fundamental que os logs gerados sejam protegidos de alteração e deleção.

Para manuseio, troca e armazenamento de dados não deve ser permitido ao colaborador a extração indevida de informações, sem que seja formalizado um pedido, e aprovado pela Diretoria Executiva - CTO. Exceções devem ser deliberadas, somente, pela Diretoria Executiva - CTO.

5.15. Conscientização e Divulgação

5.15.1. Contratação e Movimentação de Pessoas

Todos os colaboradores contratados - devem tomar conhecimento desta Política e cumprir todas as regras descritas, o mesmo tratamento deve ser dado ao Código de Ética e Conduta e o Termo de Responsabilidade para acesso à Rede Warren, assumindo o dever sobre sigilo, mesmo quando desligado, das informações relacionadas aos sistemas, processos e operações.

O Termo de Responsabilidade deve ser assinado pelos colaboradores e deve ser revisto sempre que ocorrer alteração no contrato (de prestadores de serviços de TI ou de terceiros contratados de TI), bem como no processo de desligamento do colaborador.

A Área de Pessoas e Cultura deve controlar, junto aos colaboradores, o processo de certificação e recertificação, atentando-se:

- Ao prazo do certificado, evitando que o colaborador execute suas atividades utilizando certificados vencidos;
- Certificação PQO e equivalências com outras certificações, conferindo à área em que o colaborador está alocado e, também, à respectiva atividade executada.

5.15.2. Propriedade Intelectual

O colaborador deve ter ciência que, os direitos de autoria e propriedade intelectual relativos aos programas de computador, sistemas e demais suportes tecnológicos a que vier ter acesso e/ou desenvolver durante a vigência de seu vínculo profissional, pertencem exclusivamente à Instituição.

Ficando certo que, a compensação relacionada ao trabalho do colaborador, associada à pesquisa e ao desenvolvimento, está vinculada somente à remuneração contratual acertada.

5.15.3. Processo – Mesa Limpa e Tela Limpa

Os processos mesa limpa e tela limpa asseguram que as informações sensíveis, tanto em formato digital quanto físico, e ativos (notebooks, celulares, tablets, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período ou ao final do dia. Seguem demais ações que auxiliam neste processo:

- Computadores pessoais e terminais de computador não devem ser deixados logados, caso o responsável não esteja presente.

- Destruir os documentos impressos antes de jogá-los. Sempre que possível utilizar máquinas fragmentadoras. Caso não haja informações confidenciais, utilizar o verso ou as partes em branco da folha como rascunho.

Essas ações visam a sustentabilidade e a redução do risco de violação de segurança, fraudes e roubos de informações.

5.15.4. Programa de Conscientização

O programa de conscientização tem como objetivo capacitar e sensibilizar colaboradores, estagiários e terceiros quanto às boas práticas de Segurança da Informação, Segurança Cibernética e Segregação de Funções, promovendo a disseminação do conhecimento e a construção de uma cultura organizacional orientada à segurança.

O conteúdo do programa é atualizado e aplicado anualmente, sendo composto por:

(i) Treinamento em vídeo e consulta do material em PDF com o objetivo de apresentar:

- Conceitos de Segurança da Informação, Segregação de Funções e Cibernética e contribuir com a disseminação de informações e transferência de conhecimentos na Instituição.
- Princípios da tecnologia da informação;
- Configuração de senhas;
- Uso dos canais de comunicação; e
- Proteção do ambiente corporativo.

(ii) Avaliação, ao final do curso para medir a aderência mínima esperada ao final do treinamento.

- Novos colaboradores devem concluir o curso em até 14 dias após o início do vínculo com a Instituição.
- A Diretoria de Gente e Gestão é responsável por monitorar o progresso e garantir o cumprimento do prazo.
- O conteúdo é disponibilizado durante a agenda de boas-vindas e na plataforma de *onboarding* institucional.
- Para os colaboradores já ativos, o treinamento é realizado anualmente, com leitura obrigatória do material e realização de avaliação ao final do ciclo.
- Para aprovação, é necessário atingir mínimo de 70% de acerto na avaliação.

(iii) Planos de ação para conscientização daqueles que não atingirem o resultado mínimo esperado.

- Os colaboradores que não atingirem o percentual esperado poderão realizar aprova novamente (reavaliação);

- Adicionalmente, deverão participar de treinamento realizado pela área de Compliance que abordará as melhores práticas em relação ao tema.

5.15.5. Pílulas Semanais de Conscientização

São divulgadas semanalmente, por meio do Slack corporativo, mensagens educativas com dicas práticas de segurança da informação, baseadas nas recomendações da cartilha do CERT.br. Os temas abordam boas práticas digitais, proteção de dados pessoais e corporativos, prevenção a golpes e fraudes, entre outros tópicos relevantes.

5.15.6. Campanhas de Phishing Simulado

Duas vezes ao ano, são realizadas campanhas internas de phishing simulado. Os colaboradores que clicarem no link malicioso (simulado) deverão obrigatoriamente realizar uma avaliação de reciclagem sobre Segurança da Informação, com foco em phishing e boas práticas relacionadas.

A avaliação exige um mínimo de 80% de acerto para aprovação. Aqueles que não atingirem o índice mínimo devem refazer a avaliação até alcançar a pontuação exigida.

Essas ações visam garantir a atualização contínua do conhecimento sobre segurança cibernética e reduzir o risco de incidentes causados por engenharia social ou falhas humanas.

5.15.7. Guia de boas práticas

A Warren Rena, em conformidade com a regulamentação vigente e com seu compromisso com a segurança cibernética, disponibiliza em sua rede mundial de computadores (website institucional) orientações atualizadas sobre as principais práticas de segurança da informação, contemplando, no mínimo:

I – Práticas adotadas pela Warren Rena quanto:

a) aos controles de acesso lógico aplicados aos clientes; e

b) à proteção da confidencialidade dos dados cadastrais, operações e posição de custódia de seus clientes; e

II – Cuidados recomendados aos clientes no uso dos sistemas providos pela Warren Rena.

5.16. Gerenciamento de Sessões – Gerenciamento de Sessões – Plataforma da Corretora

Com o objetivo de mitigar riscos relacionados ao uso indevido de sessões ativas em nosso aplicativo, a Companhia estabelece as seguintes diretrizes para o gerenciamento de sessões na plataforma da corretora:

Sessão ativa (com interação contínua do usuário):

A sessão deverá expirar automaticamente após 12 horas de uso contínuo, mesmo com interação do usuário, como medida preventiva para evitar sessões excessivamente longas e reduzir a exposição a riscos.

Sessão inativa (sem interação do usuário):

A sessão deverá ser encerrada automaticamente após um período máximo de 30 minutos de inatividade, considerando o risco de acesso indevido em dispositivos desbloqueados ou compartilhados.

Essas diretrizes aplicam-se exclusivamente à plataforma digital da corretora disponibilizada aos clientes, e visam garantir o equilíbrio entre segurança da informação e usabilidade, assegurando a proteção dos dados e das credenciais dos usuários finais.

6. Diretor Responsável

O Diretor Estatutário responsável pela Política de Segurança da Informação e Cibernética, bem como pela execução do Plano de Ação e de Resposta a Incidentes, é Bruno Fonseca.

Compete a esse diretor aprovar, implementar, supervisionar e assegurar o cumprimento desta Política, em conformidade com a Resolução BCB nº 85/2021 e demais normativos aplicáveis.

7. Exceção às Regras estabelecidas Neste Instrumento Normativo

Em havendo qualquer exceção relacionada às regras e diretrizes estabelecidas nesta Política, esta deverá ser aprovada, em primeira instância, pela Diretoria Executiva – CTO e Diretoria de Compliance.

8. Papéis e Responsabilidades

Diretoria Executiva

- Aprovar a Política de Segurança da Informação, em consonância com as regulamentações vigentes;
- Estabelecer decisões administrativas referentes aos casos de descumprimento desta Política;
- Comprometer com as melhorias contínuas dos procedimentos relacionados neste documento.

Área de Segurança da Informação

- Assegurar a efetividade e continuidade da aplicação desta Política;
- Garantir que medidas corretivas sejam adotadas quando falhas de conformidade forem identificadas;
- Garantir a proteção adequada das informações e dos sistemas contra acesso indevido, cópia, leitura, modificação, destruição e divulgação não autorizados;
- Assegurar que os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela Instituição, estando sujeitos à monitoração, rastreabilidade e auditoria;
- Assegurar, juntamente com a Diretoria de Compliance, que a Política esteja em conformidade com as regulamentações vigentes;

- Emitir parecer acerca das ações a serem implementadas para correção das deficiências apontadas;
- Proteger continuamente todos os ativos de informação da Instituição contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado
- Orientar as áreas e gestores a respeito dos procedimentos e práticas a serem cumpridas;
- Desenvolver e aplicar procedimentos e ações que visam garantir a disponibilização da informação de forma íntegra e segura;
- Adotar postura crítica quanto aos riscos envolvidos, evidenciada por meio de ambientes de controle, com o objetivo de propor planos de ação para a melhoria dos processos, visando à mitigação de possíveis impactos ao Grupo Warren;
- Executar a revisão necessária, de forma que sejam evitadas ausências relacionadas à aplicação do software antivírus no Parque Tecnológico da Instituição;
- Executar os controles relacionados ao teste diário de conectividade (relativo aos testes matinais), visando a atendimento à governança estabelecida e aos Órgãos Reguladores;

Área de Gente e Gestão

- Informar de maneira imediata as áreas envolvidas sobre contratação, desligamento, afastamento e modificações no quadro de colaboradores, visando garantir a execução dos procedimentos necessários;
- Disponibilizar o Termo de Responsabilidade e Ciência aos novos colaboradores, no ato da contratação, para ciência e assinatura, visando o comprometimento junto às regras estabelecidas nesta Política.
- Garantir que os colaboradores e prestadores de serviços realizem os treinamentos obrigatórios.
- Garantir que os colaboradores e prestadores de serviços estejam com suas respectivas certificações atualizadas e em conformidade com a determinação do Autorregulador e Regulador.

Área Jurídica

- Observas as cláusulas contratuais na contratação de prestadores de serviços e parteiros conforme estipulado nesta Política;

Área de Compliance

- Garantir que as regras estabelecidas nesta Política estejam de acordo com o determinado pela Direção Executiva e regulamentações vigentes;
- Avaliar em conjunto com as Áreas de Controles Internos e Gerência de Segurança da Informação os riscos relacionados à segurança da informação e apresentar propostas de aperfeiçoamento da conformidade junto ao Auto Regulador e Regulador, quando for o caso.
- Fazer, por meio de disseminação do conteúdo, com que todos os colaboradores, prestadores de serviços de TI e terceiros contratados de TI tenham conhecimento deste documento;
- Manter esta Política devidamente atualizada, juntamente com as Áreas de Controles Internos e Gerência de Segurança da Informação;
- Caso sejam constatadas quaisquer atipicidades, conduzir investigações internas e sigilosas, verificando se há indícios de irregularidades, de modo a combatê-las com base nas boas práticas e determinações de governança.

Colaboradores e Terceiros Prestadores de Serviços Vinculados ao Grupo Warren

- Informar à gestão imediata e à Gerência de Segurança da Informação qualquer ação que não condiz com o determinado nesta Política;
- Zelar pela segurança de suas credenciais de acesso (senha, múltiplo fator de autenticação, e chaves privadas) de todos os ativos de informação que tiver acesso, 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;
- 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;
- Cumprir integralmente as regras determinadas nesta Política.

9. Documentos Vinculados

Esta Política de Segurança da Informação é complementada por um conjunto documentos que devem ser observados de forma integrada.

São eles:

- Política de Privacidade e Proteção de Dados;
- Política de Backup e Restore;
- Política de Gestão de Mudança;
- Política de Gestão de Continuidade de Negócios;
- Política de Seleção, Supervisão e Contratação de Terceiros;
- Procedimento de Segregação de Funções e Controles de Acessos;
- Procedimento de Prevençao Contra Vazamento de Dados;
- Procedimento de Monitoramento Infraestrutura;
- Guia de Boas Práticas de Segurança da Informação;

10. Vigência

Esta Política entra em vigor na data da sua publicação e dever ser revisada, no mínimo, anualmente, bem como quando ocorrerem alterações significativas nos processos definidos neste documento.