Política de Segurança da Informação

cDocCode

Tipo de Documento	Área	Título	Criticidade
cDocType	cDocArea	cDocTitle	cCrit

Código	Revisão	Autor(a)	Revisor(a)	Aprovador(a)	Data de Aprovação
cDocCode	cDocRev	cAuthor	cReviewer	Conselho PRIO	cDataAprovAtual

Unidades Aplicáveis		
cAUnit1	cAUnit2	cAUnit3
cAUnit4	cAUnit5	cAUnit6
cAUnit7	cAUnit8	cAUnit9

Controle de Revisões

Revisão	Data de Aprovação	Descrição
cDocRev0	cDataAprov0	cRevDesc
cDocRev1	cDataAprov1	cRevDesc1
cDocRev2	cDataAprov2	cRevDesc2
cDocRev3	cDataAprov3	cRevDesc3
cDocRev4	cDataAprov4	cRevDesc4
cDocRev5	cDataAprov5	cDocRev5
cDocRev6	cDataAprov6	cDocRev6
cDocRev7	cDataAprov7	cDocRev7
cDocRev8	cDataAprov8	cRevDesc8
cDocRev9	cDataAprov9	cRevDesc9

SUMÁRIO

1. OBJETIVOS 5
2. APLICAÇÃO E ALCANCE 5
3. DEFINIÇÕES E ABREVIATURAS 5
4. RESPONSABILIDADES 6
5. INSTRUÇÕES DE SEGURANÇA (NÃO APLICÁVEL) 8
6. EQUIPAMENTOS NECESSÁRIOS (NÃO APLICÁVEL) 8
7. DESCRIÇÃO 8
7.1. Pilares da Segurança da Informação 8
7.2. Disposições Gerais 8
7.3. Propriedade e Classificação das Informações 9
7.4. Segurança na Gestão de Pessoas 11
7.5. Gestão de Identidade Corporativa 11
7.5.1. Utilização de Contas e Senhas 11
7.5.2. Gestão do Ambiente de Trabalho 12
7.5.3. Utilização de Eletrônicos e Mídias Móveis 12
7.6. Gestão de Acessos 13
7.6.1. Recursos de TI 13
7.6.2. Acesso Lógico 13
7.6.3. Acesso Físico 13
7.7. Utilização da Rede e de Aplicações 13
7.7.1. Redes e Aplicações 13
7.7.2. Desktops e Notebooks 14
7.7.3. Acesso Remoto 14
7.7.4. Acesso à Internet 14
7.7.5. Correio Eletrônico e Mensageria 15
7.7.6. Telefonia Convencional 16
7.7.7. Controle de Softwares e Aplicações 16
7.8. Gestão de Ativos 16
7.8.1. Gestão de Ativos 16
7.8.2. Controle dos Ativos 17
7.8.3. Utilização Externa de Equipamentos 17
7.9. Backup das Informações 17
7.10. Gestão de Incidentes 17
7.10.1. Notificação de Eventos e Incidentes 17
7.11. Privacidade e Proteção de Dados 18
7.12. Disposições Finais 18
8. ANEXOS 18
9. REFERÊNCIAS 18

9.1. Internas 19

Índice de Ilustrações

Figura 1: Pilares da Segurança da Informação. 8

Índice de Tabelas

Tabela 1: Classificação das Informações. 10

1. OBJETIVOS

A presente Política ("Política") visa estabelecer e difundir os pilares e as diretrizes da Política de Segurança e Informação da PRIO S.A., inclusive de suas sociedades controladas, direta ou indiretamente, no Brasil ou no exterior ("Sociedades Controladas", em conjunto com a Companhia, "PRIO").

O seu objetivo é assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações, visando proteger a PRIO, sua imagem, reputação e a continuidade de seus negócios, bem como seus Colaboradores, Terceiros Alocados, e Parceiros de Negócios.

2. APLICAÇÃO E ALCANCE

Esta Política deve ser conhecida e observada pelos Colaboradores da PRIO. Ela também se aplica aos Terceiros Alocados e Parceiros de Negócio, que se relacionam, direta ou indiretamente, com a Companhia, independentemente da natureza da relação, se continuada ou pontual, se envolve a transferência de recursos financeiros ou apenas de conhecimento (know-how).

As diretrizes estabelecidas nesta Política devem ser aplicadas globalmente, ainda que a respectiva legislação local tenha regras mais brandas e, portanto, admita ou tolere algumas condutas diferentes das aqui definidas. Em casos de conflito entre esta Norma e a legislação local, a norma mais protetiva deverá ser aplicada.

3. DEFINIÇÕES E ABREVIATURAS

A fim de facilitar a compreensão e interpretação desta Norma, são apresentados abaixo os seguintes conceitos e siglas, os quais devem ser entendidos tanto na forma singular quanto na forma plural:

- **Aparelhos Eletrônicos**: Dispositivos que podem ser ligados a rede de dados. Exemplo: Celular e Tablet.
- **Ativos Físicos**: São todos os prédios, veículos, mobiliário, computadores, telefones, material de escrita e similares tipicamente utilizados por Colaboradores da PRIO na fiel execução do seu trabalho.
- **Ativos Lógicos**: São os softwares utilizados pelos colaboradores através de computadores, dispositivos móveis, smartphones e similares.
- **Colaborador**: Toda pessoa física que tenha vínculo empregatício direto ou estatutário com a PRIO. Inclui, além do empregado contratado sob o regime da Consolidação das Leis do Trabalho -CLT no Brasil, aqueles contratados sob leis estrangeiras ou outros regulamentos correspondentes, estagiários, menores aprendizes, empregados temporários e membros de comitês, estatuários ou não.

- **ERP (Enterprise Resource Planning ou Planejamento dos Recursos da Empresa)**: Sistema responsável por cuidar de todas as atividades diárias de uma empresa, do administrativo ao operacional. Ex.: Protheus e SAP.
- **GTI**: Gerência de Tecnologia da Informação.
- **Informação**: A informação pode existir em diversos formatos, tais como: impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos, mostrada em filmes ou falada em conversas. Independentemente da forma apresentada ou do meio através do qual a informação é compartilhada ou armazenada, ela deve estar protegida de acordo com as diretrizes corporativas de Segurança da Informação.
- **Mídias Removíveis**: Tipo de memória que pode ser removida do seu aparelho de leitura, conferindo portabilidade para os dados que carrega. Ex.: Pen Drive, HD portátil, CD\DVD.
- **Parceiro de Negócios**: Qualquer pessoa, física ou jurídica, com a qual a PRIO tenha parceria comercial (e.g., fornecedores de material e/ou serviços, clientes, empresas consorciadas), técnica, social ou institucional.
- **Recursos de TI**: são todos os Ativos Físicos e Lógicos utilizados para gerenciar, processar, armazenar e transmitir informações dentro de uma organização. Isso inclui hardware, software, redes, sistemas de gestão de dados, serviços de nuvem, dispositivos móveis, aplicativos, servidores, sistemas de segurança da informação, e quaisquer outras ferramentas tecnológicas que suportam as operações e processos de negócios.
- **SCADA (Sistemas de Supervisão e Aquisição de Dados)**: Toda infraestrutura de software e hardware utilizado para monitorar e supervisionar as variáveis e os dispositivos de sistemas de controle de automação conectados através de servidores/drivers de comunicação (drivers) específicos.
- **Terceiro Alocado**: Toda pessoa física ou jurídica que não tenha vínculo empregatício, mas que preste serviços de natureza não eventual (rotineira) e remunerada à PRIO. Também inclui o consultor, portador de um CNPJ próprio, contratado diretamente pela PRIO para a execução de uma função por tempo determinado, física ou remotamente, sob regras contratuais especificadas em contrato de prestação de serviço específico.
- **Usuário**: É todo e qualquer Colaborador, Terceiro Alocado ou visitante que utilize os Recursos de TI disponibilizados pela PRIO.

4. RESPONSABILIDADES

Visando assegurar um ambiente de trabalho seguro, a PRIO estabelece as seguintes responsabilidades:

Colaboradores e Terceiros Alocados abrangidos por esta Política:

- Cumprir as regras desta Política de Segurança da Informação;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados;
- Assegurar que os Recursos de TI, as informações e os sistemas a sua disposição sejam utilizados apenas para as finalidades de negócio;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual, bem como os documentos correlatos da PRIO;
- Não discutir, citar ou compartilhar assuntos confidenciais em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo comentários e opiniões em blogs e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo; e
- Comunicar imediatamente à GTI qualquer descumprimento ou violação desta Política e/ou de suas normas e procedimentos.

Pessoas e Performance

- Comunicar a GTI sobre a admissão, mudança de departamento, afastamento temporário ou permanente, ou desligamento de um Colaborador ou Terceiro Alocado com acesso a Recursos de TI.
- Coordenar a assinatura e coleta de Termo de Adesão previsto no anexo I desta Política.
- Aplicar e evidenciar treinamentos de Segurança da Informação, devendo seus registros serem armazenados conforme a legislação.

Gestores:

- Comunicar a GTI sobre o perfil de acesso de Colaboradores ou Terceiro Alocados, inclusive para a sua devida liberação, alteração, suspensão ou revogação de acesso a Recursos de TI.
- Reforçar e orientar os Colaboradores e Terceiros Alocados sob sua gestão em relação a práticas, processos de segurança, acessos a sistema e diretrizes dispostas nesta Política.

GTI:

- Promover ampla divulgação desta Política e monitorar a sua devida aplicação;
- Promover ações de conscientização sobre segurança da informação para os Colabores, Terceiros Alocados e Parceiros de Negócio, quando aplicável;
- Propor ações de aperfeiçoamento da segurança da informação; e
- Estabelecer normas e procedimentos relacionados à instrumentação da segurança da informação, dispondo sobre a propriedade e o uso da informação, a gestão de acessos e identidades e os incidentes de segurança da informação.

5. Instruções de Segurança (Não aplicável)

6. Equipamentos Necessários (Não aplicável)

7. Descrição

7.1. Pilares da Segurança da Informação

Figura 1: Pilares da Segurança da Informação

São pilares da Segurança da Informação:

- **Disponibilidade**: Característica das informações que podem ser acessadas por pessoas autorizadas quando necessário às atividades do negócio.
- **Integridade**: Característica das informações que somente são alteradas por pessoas autorizadas através de processos documentados.
- **Confidencialidade**: Característica das informações que estão disponíveis somente para pessoas autorizadas ou sistemas corporativos.
- **Segurança da Informação**: Ausência de incertezas baseada nos 3 (três) Pilares.

7.2. Disposições Gerais

A informação é um ativo valioso e crucial para a Companhia, essencial para o sucesso de seus negócios, e, por isso, merece proteção adequada. A segurança da informação envolve a adoção de medidas para proteger a propriedade, confidencialidade, disponibilidade e integridade da informação, seja em formato físico ou digital, contra diversas ameaças, visando evitar seu uso indevido, inadequado, ilegal ou em desacordo com as políticas e procedimentos internos. Para isso, devem ser seguidas as diretrizes indicadas a seguir.

Para o fiel cumprimento desta Política é esperado de Colaboradores e Terceiros Alocados a serviço da PRIO:

- Aplicar os controles definidos no item de “Classificação das Informações”.
- Zelar pela Segurança das Informações da empresa e de seus parceiros comerciais, informando imediatamente qualquer incidente de segurança da informação ou violação, intencional ou não, das regras descritas na Política de Segurança da Informação ao superior imediato ou a Área de Segurança da Informação.
- Acessar a rede corporativa, correio eletrônico corporativo e Sistemas de Informação somente por necessidade de serviço, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas nas normas internas da PRIO.
- Zelar pela integridade, confidencialidade e disponibilidade dos dados, informações contidas nos sistemas, e da infraestrutura de tecnologia da informação a que tenha acesso, devendo comunicar por escrito aos responsáveis, de quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas nos sistemas e na infraestrutura de tecnologia da informação, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes, sob pena das sanções previstas neste instrumento.

Todos os Colaboradores, Terceiros Alocados e Parceiros de Negócios da PRIO, como também as entidades que possuem acesso às informações ou às instalações e infraestrutura da Companhia devem conhecer os termos desta Política, as normas pertinentes ao desenvolvimento de seu trabalho e o Código de Ética e Conduta da empresa.

Os contratos com empresas prestadoras de serviços que possuem acesso às informações, aos sistemas e/ou ao ambiente da Companhia devem incluir cláusulas que garantam o cumprimento das regras de segurança da informação, bem como penalidades em caso de descumprimento.

7.3. Propriedade e Classificação das Informações

As informações produzidas pelos Colaboradores e Terceiros Alocados a serviço da PRIO são de propriedade exclusiva da Companhia, independentemente de seu formato ser físico ou digital. Da mesma forma, a PRIO também é proprietária das informações disponibilizadas à Companhia, de maneira autorizada, por terceiros, e essas informações devem ser utilizadas exclusivamente para o atendimento dos objetivos do negócio.

Toda informação deverá ser classificada de acordo com seu nível de confidencialidade, seguindo os seguintes parâmetros:

Nível de Classificação	Descrição
Pública	A informação pode ou deve ser divulgada publicamente sem que isto acarrete qualquer dano à organização, incluindo funcionários, clientes, fornecedores, imprensa e público em geral.
Interna	É toda informação interna a qual sua divulgação pode causar pequeno constrangimento ou inconveniência operacional.
Restrita	É toda informação restrita, a qual poderá gerar impacto significante a curto prazo nas operações ou objetivos táticos da organização se divulgada indevidamente.
Confidencial	É toda informação de alto nível de sensibilidade e criticidade, a qual poderá gerar um sério impacto nos objetivos de longo prazo ou risco à sobrevivência da organização se divulgada indevidamente.

Tabela 1: Classificação das Informações

A esse respeito é ressaltado que:

- Toda informação será considerada confidencial quando associada a interesses estratégicos, de negócios e/ou financeiros da PRIO, bem como informações de dados pessoais ou sensíveis. Caso revelada, pode trazer prejuízos financeiros, impactos ao negócio ou repercussões negativas à imagem da PRIO.
- A informação classificada como “Confidencial” deve indicar quais pessoas, ou grupos de pessoas, podem acessá-la.
- É de responsabilidade do gestor da área a classificação das informações e apenas este, ou seus superiores hierárquicos, pode alterar a classificação de uma informação.
- Todo colaborador possui a responsabilidade de comunicar imediatamente a GTI sobre toda e qualquer violação que ofereça risco de vazamento de informações.
- Exemplos de informações confidenciais:
  - ✓ Planejamento Estratégico da PRIO;
  - ✓ Tabela de Cargos e Salários;
  - ✓ Dados dos Clientes e Fornecedores;
  - ✓ Dados de Operação;
  - ✓ Dados do Sistema ERP (exemplo: Protheus e Portal RH);
  - ✓ Chaves Criptográficas;
  - ✓ Senhas de Acesso aos Sistemas.
  - ✓ Dados pessoais e dados pessoais sensíveis.
  - ✓ Informações sobre sísmica, geologia de poços, métodos e técnicas de exploração.

Os equipamentos, meios de comunicação e sistemas da PRIO estão sujeitos a monitoramento, e qualquer informação de cunho pessoal tratada por esses meios ou fornecida à Companhia será incluída nesse controle. Todos os Colaboradores e Terceiros Alocados abrangidos por esta Política estão cientes desse monitoramento.

7.4. Segurança na Gestão de Pessoas

Todo Colaborador deve receber treinamento operacional antes de iniciar suas atividades técnicas, salvo nos casos em que o funcionário tenha o conhecimento e a experiência necessários comprovados, objetivando minimizar o risco de falhas em procedimentos operacionais da cadeia de valor da PRIO. O mesmo procedimento deve ser aplicado aos Terceiros Alocados a serviço da PRIO.

No ato da contratação do Colaborador e Terceiro Alocado, este deve ser comunicado dos seus papéis e responsabilidades pertinentes a segurança da informação, devendo ser coletada a ciência quanto ao disposto na Política de Segurança da informação.

Este procedimento será realizado por meio do preenchimento do Termo de Adesão previsto no Anexo I desta Política. A responsabilidade pela assinatura será do Colaborador ou Terceiro Alocado. Enquanto, caberá ao time de Pessoas e Performance coordenar a assinatura e coleta do documento junto aos Gestores, para posterior entrega a GTI.

Todo colaborador deve receber o treinamento básico em Segurança da Informação na primeira Integração após sua contratação. Este treinamento deve ser aplicado, evidenciado, devendo tais registros ser armazenados conforme a legislação pelo time de Pessoas e Performance.

A Área de Segurança da Informação deve efetuar atividades de treinamento e conscientização no mínimo a cada 12 (doze) meses. A participação é obrigatória a todos os colaboradores e aos terceiros que acessam informações confidenciais.

7.5. Gestão de Identidade Corporativa

7.5.1. Utilização de Contas e Senhas

A identificação de acesso aos Recursos de TI deve ser efetuada através de uma conta (login) e uma senha, pessoal, ambas intransferíveis, criadas originalmente pela GTI e atualizadas, conforme for o caso, pelo Colaborador ou Terceiro Alocado, mediante a observância das diretrizes dessa Política para garantir a segurança do acesso e da utilização dos recursos.

As contas (logins) e senhas fornecidas aos colaboradores são de uso individual e intransferível, sendo vedado ao titular compartilhá-los ou fornecê-los a terceiros. Caberá ao colaborador adotar as medidas cabíveis para que as credenciais permaneçam de seu único conhecimento. As senhas de acesso são classificadas como informação confidencial.

Os colaboradores são responsáveis por todas as ações realizadas mediante as contas e senhas que lhes são atribuídas. As senhas de acesso devem ser alteradas em intervalos de 90 (noventa) dias. É proibida a reutilização das últimas 10 (dez) senhas válidas.

As senhas de acesso devem possuir autenticação de duplo fator e ser compostas por, no mínimo, 8 (oito) caracteres alfanuméricos, devendo conter ao menos 1 (um) caractere minúsculo 1 (um) maiúsculo, 1 (um) numérico e 1 (um) de pontuação (especial).

Por sua vez, as senhas de acesso às contas administrativas, devem possuir autenticação de duplo fator e ser compostas por, no mínimo, 12 (doze) caracteres alfanuméricos, devendo conter ao menos 1 (um) caractere minúsculo 1 (um) maiúsculo, 1 (um) numérico e 1 (um) caractere de pontuação (especial). É proibida a reutilização das últimas 24 (vinte e quatro) senhas válidas. O Usuário será bloqueado após 5 (cinco) tentativas de acesso, devendo aguardar 30 (trinta) minutos para nova tentativa.

As senhas deverão ser alteradas sempre que obrigatório ou mediante suspeição de descoberta por terceiros. Devem ser evitadas combinações simples que possam ser facilmente descobertas. Além disso, as senhas padrões predefinidas ou fornecidas pelos fornecedores deverão ser alteradas imediatamente após a instalação de sistemas ou softwares.

O Colaborador e o Terceiro Alocado não poderão utilizar a mesma senha para serviços e sistemas distintos.

O colaborador e o Terceiro Alocado responderão, em todas as instâncias, pelas consequências das ações ou omissões de sua parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de logins e senhas ou das transações a que tenha acesso.

7.5.2. Gestão do Ambiente de Trabalho

Impressões, cópias, mídias magnéticas ou óticas e outros documentos ou dispositivos físicos que armazenem informações confidenciais devem ser recolhidos imediatamente e armazenados física ou logicamente.

Deve ser mantida a necessária cautela quando da exibição de informações em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que pessoas não autorizadas venham a tomar ciência das informações ali presentes.

Informações que não sejam mais necessárias para uso contínuo, eventual, ou que extrapolarem o período de retenção legal, devem ser descartadas.

7.5.3. Utilização de Eletrônicos e Mídias Móveis

O uso de aparelhos eletrônicos corporativos móveis, como celulares e tablets, para acesso às informações é livre, desde que observada a classificação da informação acessada pelo Colaborador ou Terceiro Alocado. Por sua vez, os Recursos de TI da PRIO somente poderão ser acessados por aparelhos eletrônicos e/ou mídias removíveis pessoais após aprovação da GTI.

Os celulares, tablets e notebooks que possuírem acesso ao correio eletrônico corporativo receberão os controles listados nesta Política.

7.6. Gestão de Acessos

7.6.1. Recursos de TI

É responsabilidade da área de Pessoas e Performances comunicar a GTI sobre a admissão, mudança de departamento ou desligamento de um Colaborador ou Terceiro Alocado. Subsidiariamente, cabe aos gestores das diferentes áreas da PRIO informar sobre o perfil de acesso desta pessoa, inclusive para a sua devida liberação, alteração, suspensão ou revogação pela GTI.

Para garantir o controle sobre os privilégios de acesso de Colaboradores e Terceiros Alocados, qualquer afastamento, seja ele temporário ou permanente, incluindo a mudança de departamento de atuação, deverá ser informado, formalmente pela área de Pessoas e Performance, ou, subsidiariamente, pelos Gestores dos departamentos envolvidos, para que sejam tomadas as medidas cabíveis quanto ao cancelamento ou suspensão provisória e permissão do acesso.

Toda solicitação de acesso aos Recursos de TI deverá ser documentada formalmente e justificada quanto à sua real necessidade.

Os acessos concedidos a Terceiros Alocados deverão ter caráter provisório. A depender da natureza da contratação, os acessos serão concedidos pelo prazo de 3 (três) meses, sendo obrigatório ao Gestor responsável pelo mesmo aprovar a renovação do acesso.

7.6.2. Acesso Lógico

Os acessos às aplicações e à rede corporativa devem ser liberados somente mediante identificação e autenticação do Colaborador ou Terceiro Alocado. Os acessos às informações e aos ativos devem ser baseados nas necessidades de negócio, sempre considerando o perfil funcional dos Usuários.

A PRIO manterá atualizado lista dos Usuários criados, inclusive com os respectivos perfis de acesso.

O ato de logon e logoff na rede e nos ativos que armazenem informações confidenciais deve ser registrado e armazenado por 90 (noventa) dias.

As sessões locais ociosas serão automaticamente bloqueadas após 7 (sete) minutos de inatividade.

As sessões remotas ociosas serão automaticamente desconectadas após 7 (sete) minutos de inatividade.

7.6.3. Acesso Físico

O acesso às áreas classificadas como confidenciais é restrito aos Colaboradores e Terceiros Alocados, esses últimos quando especificamente autorizados pelos gestores.

7.7. Utilização da Rede e de Aplicações

7.7.1. Redes e Aplicações

As ferramentas corporativas são de uso exclusivo para o desenvolvimento das atividades profissionais e de acordo com os interesses da PRIO.

A área de Segurança da Informação pode acessar registros, sistemas e quaisquer informações existentes nos ambientes da PRIO, para investigação de fatos.

7.7.2. Desktops e Notebooks

Os Colaboradores e os Terceiros Alocados com acesso a Recursos de TI devem encerrar ou bloquear a sessão da estação de trabalho sempre que se ausentarem do local de trabalho.

Apenas a GTI poderá adicionar, alterar ou remover equipamentos e softwares em estações de trabalho, servidores e outros ativos da empresa. Em nenhuma hipótese, os padrões definidos ou os mecanismos de segurança fornecidos pela PRIO poderão ser alterados ou desativados pelos Colaboradores e Terceiros Alocados.

Apenas softwares homologados e licenciados devem ser instalados nas estações de trabalho e servidores da empresa.

É vedada a cópia de softwares, adquiridos ou desenvolvidos pela PRIO, salvo em casos excepcionais e com a expressa autorização da GTI.

7.7.3. Acesso Remoto

O acesso remoto à rede corporativa deve ser realizado exclusivamente por meio das ferramentas homologadas para este fim. Esse acesso é previamente autorizado para atividades de suporte e monitoramento de serviços críticos, desde que realizado pelas áreas responsáveis por essas tarefas, assim como por coordenadores, gerentes e diretores, seguindo perfis pré-estabelecidos. Os demais acessos devem ser avaliados pela área de Segurança da Informação. É proibido o acesso remoto através de protocolos sem criptografia.

É proibido o acesso remoto através de protocolos com criptografia fraca, tais como SSL e TLS 1.0, 1.1 ou 1.2, entre outros.

O acesso remoto deve ser realizado mediante:

- Criptografia do canal de comunicação (VPN);
- Autenticação de credenciais individuais;
- Vinculação da credencial a perfil de acesso previamente configurado.

É obrigatório o uso de duplo fator de autenticação para acesso à VPN.

O acesso remoto a dispositivos classificados como SCADA é proibido. A gestão deve ocorrer a partir da rede interna, usando dispositivos corporativos.

7.7.4. Acesso à Internet

Não é permitido o uso da Internet, entre outros, para:

- Download de softwares, músicas, vídeos, entre outros arquivos que não façam parte da rotina de trabalho do colaborador e/ou que possam infringir direitos autorais;

- Violar leis e acessar conteúdos incompatíveis com os valores da PRIO, tais como: pornografia, incitação à violência, pedofilia e preconceitos e/ou qualquer atividade tipificada como crime;
- Comprometer a privacidade ou o sigilo das informações de terceiros;
- Realizar acesso remoto a computadores e redes, pessoais ou corporativas, fora do controle da empresa, exceto quando autorizado;
- Praticar qualquer tipo de hostilidade eletrônica, tais como: alterar ou destruir a integridade de informações armazenadas em computadores.

É vedado o acesso a sites que não sejam considerados de interesse da empresa ou que possam comprometer sua imagem ou a segurança das informações.

O acesso deve ser realizado através dos mecanismos providos pela PRIO.

A PRIO irá monitorar regularmente o uso da Internet na empresa, a fim de preservar a integridade das informações, identificar vulnerabilidades e falhas de segurança, bem como verificar o seu uso adequado.

Os serviços disponibilizados através da Internet podem ser desativados temporariamente caso haja indício de tentativas de quebra de segurança, ou outras ações que ponham em risco a imagem ou os negócios da PRIO.

7.7.5. Correio Eletrônico e Mensageria

Os Colaboradores e Terceiros Alocados devem adotar linguagem e postura condizentes com os valores da PRIO. Não é permitido, entre outros, o envio de:

- Spam;
- Conteúdo pornográfico, incitação à violência, pedofilia e preconceitos e/ou qualquer atividade tipificada como crime;
- Informações classificadas como confidenciais sem autorização prévia do responsável pela informação.

Controles quanto ao tamanho máximo de anexos, limite de destinatários, entre outros, devem ser aplicados nos sistemas de correio eletrônico. Todas as mensagens que não atendam aos padrões estabelecidos poderão ser excluídas.

A concessão de contas de correio eletrônico deve ser realizada de acordo com os interesses da PRIO, que pode a qualquer momento os revogar.

As mensagens de correio eletrônico enviadas são de responsabilidade de seu remetente, devendo ser observado, especialmente, o conteúdo daquelas endereçadas ao ambiente externo.

A PRIO reserva-se o direito de monitorar e controlar o uso do correio eletrônico, sem a necessidade de aviso prévio.

A PRIO implementará controles de detecção e proteção contra *malware* e outras ameaças que comprometam a integridade, disponibilidade e confidencialidade das informações transmitidas de forma eletrônica.

7.7.6. Telefonia Convencional

O uso dos recursos de telefonia deve ser gerido pela GTI. Sendo que, é prerrogativa da PRIO gravar as ligações efetuadas através dos dispositivos de telefonia corporativos.

A utilização dos recursos de monitoração de chamadas é restrita, e deve ser autorizada pela Segurança da Informação, e pela gerência de Compliance ou, a depender do caso, pelo Comitê de Ética e Compliance da PRIO.

7.7.7. Controle de Softwares e Aplicações

Os processos de aquisição, desenvolvimento e manutenção de aplicações são exclusivos da gerência de Tecnologia da Informação. Não obstante, as demais gerências da PRIO podem solicitar os seguintes tipos de aplicação:

- Aplicações de gestão de equipe;
- Softwares de escritório;
- Sistemas especialistas que não acessem informações confidenciais.

O desenvolvimento de quaisquer sistemas que possam vir a gerar impactos ao negócio deve ser realizado ou acompanhado pela GTI. Sendo certo que qualquer solução técnica deve ser homologada pela gerência de Tecnologia da Informação, enquanto a análise quanto às funcionalidades dos sistemas homologadas pelos Usuários.

As solicitações para desenvolvimento ou contratação de novos sistemas devem ser encaminhadas ao GTI, que deverá observar as melhores práticas de segurança da Informação.

A GTI acionará o Encarregado de Dados para análise dos requisitos de privacidade, quando aplicável.

7.8. Gestão de Ativos

7.8.1. Gestão de Ativos

Apenas as equipes de suporte técnico podem alterar os controles implantados em estações de trabalho, servidores e demais ativos.

Os colaboradores devem assinar o termo de responsabilidade sempre que receberem ou devolverem um ativo de TI.

Os colaboradores se responsabilizam por utilizar os ativos físicos e lógicos em conformidade com esta Política, mantendo-os em perfeito estado de conservação, ficando ciente de que:

- Se o equipamento for danificado ou inutilizado por emprego inadequado, mau uso, negligência ou extravio, a empresa fornecerá novo equipamento;

- Em caso de dano, inutilização ou extravio do equipamento deverá ser feita a comunicação imediata ao setor de Tecnologia da Informação;
- Na hipótese de término de prestação de serviços ou no caso de rescisão do contrato de trabalho, devolverá o equipamento completo e em perfeito estado de conservação, considerando-se o tempo do uso dele, ao setor de Tecnologia da Informação.

7.8.2. Controle dos Ativos

Os Recursos de TI, em especial, ativos tecnológicos, hardware e software, devem ser registrados pela GTI.

A instalação de softwares somente deve ser realizada pelas equipes responsáveis pelo suporte especializado. Tal instalação deve ser realizada mediante autorização do responsável pelo ativo e aprovação pela GTI.

A PRIO poderá implantar controles sobre os ativos de interesse da empresa, limitando o seu uso em atividades de cunho pessoal do colaborador, ou executando inspeções sem prévio aviso.

As informações criadas, acessadas e alteradas através dos ativos corporativos são de propriedade da PRIO e estão sob os controles desta Política.

7.8.3. Utilização Externa de Equipamentos

Os equipamentos corporativos utilizados em ambientes externos devem ser protegidos com criptografia dos discos ou software de gestão das informações.

7.9. Backup das Informações

A PRIO manterá, regularmente e quando aplicável, cópia encriptada das informações, software e sistemas, com propósito de recuperação diante de eventual perda de dados ou sistemas.

Cópias de backup de informações, software e sistemas serão mantidas e testadas regularmente.

Serão implementados controles de proteção apropriados para garantir a integridade, disponibilidade e confidencialidade do backup.

Para garantia das cópias de segurança, os colaboradores deverão armazenar os dados em diretórios indicados pela área de segurança da informação.

7.10. Gestão de Incidentes

7.10.1. Notificação de Eventos e Incidentes

Quando houver suspeita de eventos ou incidentes de segurança, a área de segurança da informação deverá ser contatada.

A área de Segurança da Informação deve utilizar hardware e software dedicados à identificação, análise e registro de incidentes de segurança da informação.

Os incidentes relativos à Segurança da Informação serão tratados de acordo com as diretrizes a serem definidas pela PRIO em norma apartada.

Quando o incidente de segurança da informação envolver dados pessoais, a área de segurança deverá acionar a equipe de privacidade e o encarregado de dados imediatamente.

7.11. Privacidade e Proteção de Dados

Todas as ações a serem realizadas para o cumprimento desta Política também observará as diretrizes da Política de Privacidade, quando aplicáveis.

A área de segurança da informação deverá implementar medidas técnicas e organizacionais adequadas para proteger dados pessoais, em conjunto com a área de privacidade e Encarregado de Dados, quando aplicável.

7.12. Disposições Finais

A área de Segurança da Informação divulgará amplamente este documento, bem como providenciará treinamentos e ações de conscientização, de forma a conscientizar os colaboradores sobre a importância do tema para o desempenho de suas atividades.

A Segurança da Informação realizará auditoria interna anual para verificar a conformidade dos setores da empresa com esta Política.

Todas as exceções às diretrizes apresentadas na Política de Segurança da Informação devem ser tratadas pela Área de Segurança da Informação.

O descumprimento das regras previstas nesta política e em seus anexos é passível de sanções administrativas, conforme Código de Conduta e legislação brasileira vigente.

A presente Política deverá ser revisada periodicamente e sempre atualizada quando houver alteração relevante que impacte as diretrizes ora estabelecidas passando a vigorar da data da sua publicação.

8. Anexos

Anexo I – Termo de Adesão à Política de Segurança da Informação

Anexo II – Termo de Responsabilidade

9. Referências

Lista os documentos que foram consultados e auxiliaram na elaboração deste documento.

9.1. Internas

Código de Ética e Conduta;
Política de Gerenciamento de Riscos.

ANEXO I

Termo de Adesão à Política de Segurança da Informação

Eu, _____, declaro que LI, COMPREENDI e ACEITO os termos da Política de Segurança da Informação (“PSI”) e assumo o compromisso de cumpri-la integralmente.

Declaro, ainda, que fui comunicado da existência dos canais de notificação de eventos e incidentes, e me COMPROMETO a usá-los sempre que constatar infração a esta Política.

Local e Data

_____, _____de _____ de _____.

_____

ASSINATURA

_____

CPF

ANEXO II

TERMO DE RESPONSABILIDADE

PRIO COMERCIALIZADORA LTDA., com sede na Praia de Botafogo, 370 – 13º andar – Botafogo - CEP: 22.250-040, devidamente inscrita no CNPJ do MF sob o **nº 11.058.804/0001-68** denominada a seguir "**PRIO**" ou "**COMODANTE**", cede em comodato o Equipamento (como abaixo definido) ao portador(a) _____ RG nº_____, doravante designado(a) **Colaborador**, mediante os termos e condições a seguir.

O presente termo de responsabilidade tem por objeto a cessão em comodato pela Comodante ao Colaborador do Equipamento abaixo descrito:

DESCRIÇÃO DO EQUIPAMENTO	
NOME	
MODELO	
SERVICE TAG	
ACESSÓRIOS	

1) O Equipamento deverá ser utilizado única e exclusivamente para serviços relacionados às atividades desenvolvidas pelo Colaborador na PRIO.

2) O Equipamento é de propriedade exclusiva da PRIO, tendo o Colaborador apenas o direito de uso decorrente do comodato ora instituído, ficando expressamente **vedado** ao Colaborador:

(a) Instalar, manter ou utilizar quaisquer softwares ou aplicativos que não os instalados no Equipamento pela PRIO;

(b) Ceder, emprestar ou transferir, seja a que título for, o Equipamento ou os direitos do presente comodato, sendo absolutamente nulo qualquer ato praticado em violação desta disposição;

(c) Alterar, editar, ou excluir as configurações dos sistemas operacionais, em especial, os referentes à ZP3segurança e geração de logs;

(d) Alterar, bloquear, desativar ou de qualquer forma interceder no funcionamento dos softwares responsáveis pela proteção contra vírus de computador e outras vulnerabilidades de segurança instalados nos Equipamentos pela PRIO;

(e) Utilizar, salvo mediante expressa autorização da PRIO, dispositivos de armazenamento externo, nem, quando autorizada a utilização, sem a prévia verificação pela equipe de segurança da PRIO da existência de vírus ou conteúdo não permitido;

(f) Armazenar, acessar ou reproduzir quaisquer conteúdos impróprios, entre os quais, mas não limitados a, atividades ilícitas, materiais pornográficos, sites que incitem qualquer tipo de discriminação, o racismo, homofobia, intolerância de credo, xenofobia, *hacking,* entre outros; ou,

(g) Usar os equipamentos para a realização de atividades ilícitas, trabalhos paralelos, em parcerias externas ou para atividades políticas pessoais.

3) O Colaborador deverá restringir, através de senha pessoal, o acesso às informações contidas no Equipamento, sendo certo que a senha pessoal deverá ser fornecida à área de TI, mantendo-a sempre atualizada.

4) O Colaborador é responsável pelo uso e conservação do Equipamento, devendo o Equipamento ser devolvido em perfeitas condições de uso e com todos os acessórios, sem qualquer informação ou dados pessoais do Colaborador.

5) Na ocorrência de perda, furto ou roubo do Equipamento, o Colaborador deverá:

(a) comunicar imediatamente por e-mail a área de TI, para que seja providenciado o bloqueio do Equipamento;

(b) Em caso de roubo ou furto, realizar imediatamente o registro de ocorrência perante a autoridade policial, cuja cópia deverá ser anexada ao Termo de Perda/Roubo a ser entregue à área de TI;

(c) Fornecer à área de TI o Termo de Perda/Roubo devidamente preenchido e assinado;

6) Na hipótese de furto ou roubo do Equipamento, a reposição do Equipamento ocorrerá no prazo de até 20 (vinte) dias contados da entrega do Termo de Perda/Roubo devidamente preenchido à área de TI. A reposição está limitada a 1 (uma) ocorrência a cada período de 12 (doze) meses contados da assinatura do presente Termo de Responsabilidade.

7) Na ocorrência de perda do Equipamento ou de um novo furto ou roubo em prazo inferior a 12 meses, o valor do Equipamento deverá ser pago pelo Colaborador levando-se em consideração o valor de mercado depreciado do Equipamento.

8) O Colaborador autoriza desde já a Comodante a, nos termos do artigo 462, §1º, da Consolidação das Leis Trabalhistas (CLT), descontar em folha de pagamento ou no "termo de rescisão do contrato de trabalho" os valores correspondentes ao indicado no item 7 acima, bem como todo e qualquer prejuízo efetivamente causado, tanto no caso de utilização indevida do Equipamento, como também nas hipóteses de danos ocasionados ao Equipamento ou de se apossar indevidamente do Equipamento (incluindo a não-devolução quando solicitado pela Comodante).

9) O Colaborador declara ter ciência de que todas as informações geradas ou presentes no Equipamento são pertencentes à Comodante e não poderão ser utilizadas ou divulgadas para

quaisquer fins que não sejam os pertinentes às atividades profissionais exercidas por ele(a) na empresa. A Comodante, na qualidade de proprietária dos Equipamento, se reserva ao direito de a qualquer tempo inspecionar Equipamento sem prévio aviso.

10) O Colaborador é o único responsável pelo *backup* de dados pessoais porventura existentes no Equipamento, não cabendo a Comodante qualquer responsabilidade pela guarda ou por perda de tais dados.

11) O Colaborador se declara ciente das suas obrigações de confidencialidade, assumindo o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas atividades na Comodante, mesmo depois de terminado o vínculo contratual mantido com a empresa.

12) O Colaborador se declara ciente e reafirma sua concordância expressa com os direitos e obrigações previstos na Política de Segurança da Informação, bem como demais políticas e normas internas da Comodante, quer seja de seu conhecimento por relação direta de trabalho, ou através da empresa para a qual trabalha como contratado(a) ou fornecedor(a) da empresa. Reconhece ainda que é seu dever estar atualizado(a) com as normas da empresa, devendo sempre buscar as informações necessárias sobre as mesmas para o correto exercício de suas funções.

13) A violação ou o descumprimento dos compromissos assumidos neste instrumento, acarretará violação de segredo da empresa e desobediência a ordem que foi dirigida, ensejando exame da conduta sob o aspecto disciplinar na hipótese de empregado(a), ou rescisão de contrato com aplicação da cláusula de multa na hipótese de prestação de serviço terceirizado através de parceiro ou empresa fornecedora da Comodante, sem prejuízo de arcar pessoalmente com os danos morais e materiais dela decorrentes, e das sanções penais cabíveis.

14) Todas as disposições deste termo são independentes e, a eventual nulidade ou invalidade de uma disposição, não invalida as demais, permanecendo inteiramente válidas e aplicáveis.

15) Por fim, manifesta neste ato sua concordância expressa com todas as cláusulas acima, assinando o presente Termo de Responsabilidade como prova de seu livre e espontâneo aceite.

Rio de Janeiro, ___ de _____ de 202X.

_____	_____
Colaborador	PRIO COMERCIALIZADORA LTDA. Comodante

Autorizado por:

_____	_____
Tecnologia da Informação	Recursos Humanos