Política de Segurança da Informação

Orion Informática

Dezembro de 2025

Versão 1.10

ÍNDICE

Controle de versões

Data	Versão	Autor	Conteúdo / Modificação	Revisado e Aprovado por
12/05/2020	1.0	Marcelo Picchioni	Draft da política	-
21/05/2020	1.1	Paulo Cabrera	Revisão e inclusão do item “n” na Cláusula 3	-
27/04/2021	1.2	Marcelo Picchioni	Inclusão dos anexos a.1 e a.2	-
10/02/2022	1.3	Marcelo Picchioni	Controle de validade e versões do documento. Inclusão do item “o” na Cláusula 3	-
21/11/2022	1.4	Keith Nakamura	Inclusão dos itens “k” e “o”	-
08/03/2023	1.5	Claudio Moreira	Inclusão do item “p”	-
05/02/2024	1.6	Claudio Moreira	Uso de captcha	-
16/05/2025	1.7	Claudio Moreira	Adequação layout padrão Revisão item l – Acesso à Internet Inclusão item q – Papéis e Responsabilidades	-
01/12/2025	1.8	Keith Nakamura	Registro de aprovação no controle de versões	Luis Camargo
02/12/2025	1.9	Keith Nakamura	Nova seção Segregação de Ambientes	Marcelo Picchioni
04/12/2025	1.10	Jaqueline Janeri	Parágrafo sobre Procedimentos de Mesa Limpa e Controle de Acesso a Sala ADM/FIN e RH.	Marcelo Picchioni
19/12/2025	1.10	Keith Nakamura, Claudio Moreira e Jaqueline Janeri	Revisão anual do documento	Luis Camargo, Jorge Camargo e Marcelo Picchioni

1. OBJETIVO

Definir as diretrizes que nortearão as normas e padrões que tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, independentemente do meio em que ela esteja contida.

2. DIRETRIZES GERAIS

- A informação sob custódia da empresa, mesmo que pertencente a clientes ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas;
- A geração, utilização, armazenamento, manutenção, distribuição e destruição da informação deve ser feita de acordo com as necessidades da empresa, sendo que estes processos devem estar devidamente documentados;
- A ORION reserva-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em malotes, envelopes, arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais;
- Deve-se usar somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário;
- O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas;
- A informação deve ser armazenada, pelo tempo determinado pela empresa ou legislação vigente, o que for maior, e recuperável quando necessário.
- O uso de redes externas de comunicação (Internet, redes privadas, etc.) deve ser controlado através de “Firewalls externos e internos”, “Antivírus” e configurações dos sistemas operacionais que garantam que somente os recursos necessários estão disponíveis para o trabalho, sem riscos para o ambiente operacional.
- O acesso externo aos sistemas da organização quando necessário pelo pessoal de Suporte ou prestadores de serviço deve ser controlado e restrito aos serviços necessários, mantendo trilhas de utilização e restringindo–se ao mínimo necessário. A solução encontrada para cada caso deve ser formalizada e documentada.
- Sistemas aplicativos desenvolvidos dentro da organização devem ser documentados e controlados quanto a alterações ou correções feitas, com trilha do que foi feito e guarda segura da biblioteca de fontes. Toda informação necessária para eventual reconstrução dos aplicativos deve constar da documentação.

- A remessa de dados da organização, seja para atender requisitos de negócio como para viabilizar a resolução de problemas encontrados deve ser avaliada em função dos riscos e adotar procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações. O que for acordado deve ser formalizado e aprovado pelos gestores da informação envolvida.
- O mau uso acidental ou deliberado dos sistemas deve ser reduzido através da separação da administração/execução de certas funções, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no desempenho de atividades críticas do sistema. Onde for difícil a segregação, outros controles, como a monitoração das atividades, trilhas de auditoria e acompanhamento gerencial devem ser considerados.

3. DIRETRIZES ESPECÍFICAS

a) Tratamento da informação:

a 1) *O* prazo de retenção for superior ao especificado pelo fabricante para utilização do meio de armazenamento, deve-se adotar um procedimento para regravação dosNormas para tratamento da informação

- Devem ser definidas regras claras para proteção da informação contra perda, alteração e acesso por pessoas não autorizadas, seja qual for o meio em que vier a ser armazenada (magnético, correspondências, relatórios, manuscritos, etc.);
- Devem ser claramente definidos os usuários (empresas, áreas, pessoas, etc.) das informações, os direitos que cada um tem para acessá-las e os procedimentos para protegê-las do acesso por pessoas não autorizadas, independentemente da forma como estiver disponível.;
- Toda informação deve ser utilizada apenas para fins profissionais, de interesse exclusivo da empresa.
- Toda informação deve ter pelo menos uma cópia reserva ou outro procedimento eficiente para pronta recuperação em caso de perda;
- Nenhuma informação deve ser acessada, divulgada ou disponibilizada, sob qualquer pretexto, sem a devida autorização;
- É proibida a transmissão a terceiros, bem como a divulgação, reprodução, cópia, utilização ou exploração, por qualquer meio, de conhecimentos, dados, e informações de propriedade da *ORION* utilizáveis nas atividades das mesmas, sem a prévia e expressa autorização da Diretoria responsável, e das quais os funcionários venham a tomar conhecimento durante a relação empregatícia, estendendo-se tal vedação ao

período após o término do contrato de trabalho, sem prejuízo das ações de natureza penal aplicáveis ao assunto.

a 2) Recomendações para o tratamento da informação

- Os funcionários devem adotar o procedimento de obter o consentimento prévio da Diretoria responsável pela informação (gestor da informação) antes de divulgá-la, independente do meio utilizado para tal (meio magnético, correspondências, relatórios, manuscritos, etc.);
- Toda informação cujo acesso possa causar prejuízos financeiros, ou à imagem pública da ORION, ou vantagem competitiva aos concorrentes, deverá ser classificada pelos emissores, ou remetentes, como “confidencial”, “restrita” e “para uso interno”, e identificada adequadamente, qualquer que seja o meio utilizado. O método de identificação (carimbo, marca d´água, etiquetas adesivas, texto orientativo, etc.) deve ser aprovado pelo gestor da informação. No caso de correio eletrônico, existe orientação específica, conforme o item (k4);
- A pessoa que receber indevidamente uma informação, deve procurar imediatamente identificar o destino desta e encaminhá-la ao destinatário. Caso isso não seja possível, a informação deve retornar ao remetente, alertando sobre o erro no envio;
- As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo da empresa;
- Toda informação em papel, mídia digital ou qualquer outro meio de armazenamento deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas;
- As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante da área. Quando forem vendidos, devolvidos ao fabricante, enviados para manutenção ou deslocados para outros usuários, as informações neles contidas deverão ser destruídas antes da liberação do equipamento;
- Os gestores devem determinar as regras de acesso e distribuição das informações, considerando os seguintes itens:
  - Riscos inerentes às informações:
    - Acesso por pessoas não autorizadas;
    - Divulgação indevida;
    - Indisponibilidade;
    - Alteração indevida.
  - Consequências:

- Fraudes - Possibilidades de lesarem a ORION ou terceiros (clientes, fornecedores, etc.);
- Problemas legais – Possibilidades de gerar prejuízos, multas, penalidades ou embaraços à ORION, a outras Empresas, Instituições ou Pessoas Físicas;
- Perda de negócio - Possibilidade de não realizar receitas previstas ou gerar perdas nos negócios implantados ou em fase de implantação;
- Prejuízo de imagem da ORION - Possibilidades de prejudicar a imagem da ORION ou de seus funcionários;
- Problemas de recuperação - Possibilidades de gerar custos de recuperação de informações perdidas ou danificadas

b) **Segurança quanto a pessoas**

- Este item trata da segurança quanto a pessoas e tem como finalidade reduzir os riscos de erros humanos, roubo, fraude ou uso inadequado de informações e recursos da ORION.

b 1) Declaração de Responsabilidade

- É um compromisso de responsabilidade direta do funcionário para com as informações, equipamentos e outras propriedades da ORION a ele confiadas e deve ser lido e assinado quando de sua admissão;
- Este conceito deve ser utilizado também para prestadores de serviço e clientes.
  - Prestadores de Serviço: a declaração de responsabilidade deve ser uma das cláusulas do contrato conforme modelo apresentado no anexo a2.
  - Clientes: a declaração de responsabilidade deve ser uma das cláusulas do termo de adesão ao produto ou documento equivalente, se ao cliente for entregue alguma senha de acesso às informações.

b 2) Normas para Declaração de Responsabilidade*:*

- A declaração de responsabilidade deve ser lida e assinada por todos os funcionários antes de ser arquivada na respectiva pasta funcional;
- O Diretor responsável por Recursos Humanos deve garantir que todos os funcionários tenham sua declaração de responsabilidade assinada;
- Poderá ser utilizado um Termo de Responsabilidade eletrônico, mediante aprovação da Diretoria Administrativa.

c) **Segurança lógica de computadores, redes e sistemas aplicativos**

- Este item trata do controle de acesso aos sistemas e às informações pertencentes ou de posse da ORION.
- Todo sistema aplicativo define um conjunto de operações aplicáveis às informações sob seu domínio. Tipicamente estas operações são: consulta, inclusão, alteração, exclusão, liberação, etc.
- Um perfil de acesso define que operações podem ser executadas por uma certa classe de usuários, usando um tipo determinado de informação.
- Caso as operações e suas respectivas informações envolvam quantias, poderão ser criadas alçadas, que definem a quantia máxima envolvida em operações executadas por cada classe de usuários.
- As regras de acesso às informações de um sistema aplicativo devem incluir a definição dos perfis, alçadas e classe de usuários, bem como os processos operacionais a serem utilizados para sua administração e controle.

c 1) Normas para segurança lógica de computadores e redes:

- Os acessos aos serviços e dados devem estar controlados com base nos requisitos de cada negócio, devem estar claramente definidos e documentados e todos os sistemas aplicativos devem estar direcionados para a implementação e manutenção desses controles;
- Cada gestor da informação deve definir e manter atualizada uma política de acesso aos seus aplicativos.

c 2) Administração do acesso aos sistemas aplicativos:

- As informações devem ser analisadas pelos respectivos gestores da informação, de forma a permitir que sejam definidas as regras de acesso, através de perfis e alçadas.
- Os sistemas aplicativos devem possuir recursos que possibilitem a administração dos acessos, através dos perfis e alçadas definidos pelos respectivos gestores da informação.

c 3) Administração do acesso de usuários*:*

- Devem existir procedimentos formais que contemplem todas as atividades ligadas à administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a eliminação de usuários.

c 4) Controle de acesso a computadores e redes*:*

- Deve ser assegurado que usuários de computadores, conectados ou não a uma rede, não comprometam a segurança de qualquer sistema ou produto;
- O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro, pelo qual o usuário conecta-se a um determinado sistema ou rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados.
- O ambiente de Produção, de Homologação e Desenvolvimento devem estar segregados entre si, de forma a impedir acessos indevidos.

c 5) *Normas* para controle de acesso a computadores, redes e sistemas aplicativos*:*

- Um sistema efetivo de controle de acesso deve ser utilizado para autenticar os usuários. As principais características desse controle são:
  - ✓ O acesso a computadores e redes deve ser protegido por senha;
  - ✓ As senhas poderão ser alteradas pelos usuários em qualquer ambiente (operacional ou aplicativo);
  - ✓ Os sistemas devem ser programados para nunca exibir a senha na tela;
  - ✓ As senhas devem ser individuais e intransferíveis;
  - ✓ As senhas não devem ser triviais e previsíveis.;
  - ✓ Os tipos de caracteres utilizados para a formação da senha devem ser:
    - Letras maiúsculas;
    - Letras minúsculas;
    - Números, e
    - Sinais ou símbolos especiais.

    Exemplos: @ # $ % & * - + = “ ´ ` ^ ~ { } [ ] / | \ ? !
  - ✓ As senhas deverão ter um tamanho mínimo de 10 (dez) caracteres, sendo obrigatória a utilização de no mínimo três dos quatro tipos de caracteres acima definidos, sendo mandatário o uso de no mínimo um sinal ou símbolo especial;
  - ✓ Os sistemas devem prever um prazo para a expiração de senhas, de no máximo 90 (noventa) dias;
  - ✓ Caso algum sistema defina uma senha inicial, deverá obrigar o usuário a alterá-la no primeiro acesso;
  - ✓ As senhas trocadas ou expiradas devem ser cadastradas para efeito de bloqueio de reutilização (mínimo de doze senhas);
  - ✓ Os arquivos de senhas devem ser criptografados e gravados separadamente dos arquivos de dados, em ambiente de acesso restrito;
  - ✓ Os acessos não autorizados por senha inválida devem ser bloqueados após um máximo de cinco tentativas.

- ✓ A senha uma vez aprovada deve garantir acesso exclusivo do usuário na estação de trabalho. Portanto um mesmo usuário não poderá estar ativo simultâneamente em mais de uma estação de trabalho. Em algumas situações essa obrigatoriedade poderia ser suprimida, desde que devidamente documentada e esclarecida, com anuência da Diretoria Administrativa.
- ✓ A senha é de uso exclusivo e pessoal e não deve ser compartilhada, nem mesmo entre pessoas da mesma área.
- ✓ Todos os sitemas que disponibilizem o mecanismo de captcha devem ser habilitados

c 6) Monitoramento de uso e acesso aos sistemas aplicativos:

- Todos os sistemas aplicativos deverão:
  - ✓ Detectar tentativas de acesso não autorizado;
  - ✓ Registrar eventos de entrada no sistema (login) e saída do sistema (logout);
  - ✓ Sempre que houver riscos que afetem o negócio deve-se gravar trilhas de auditoria para futuras investigações, registrando os dados dos acessos, tais como: identificação do usuário, localidade, identificação do terminal ou estação de rede, data e hora do acesso, identificação do aplicativo acessado e transações executadas.
  - ✓ Emitir relatórios gerenciais de acessos (por usuário, módulo do aplicativo e funções).

d) **Segurança no acesso de Prestadores de Serviço**

- Este item visa estabelecer controles sobre recursos de processamento da informação da organização no desempenho dos serviços contratados.
- Deve ser feita uma avaliação dos riscos envolvidos para determinar as implicações de segurança e os controles necessários. O que for acordado pode ser explicitado no contrato assinado.
- Caso o prestador utilize equipamentos próprios que precisem estar conectados à rede da organização, deve-se avaliar os riscos e estabelecer controles ou impedimentos que garantam a segurança estabelecida. Se for necessário deve-se segregá-los em uma rede própria e estabelecer um “firewall” para controlar os acessos.
- O único ambiente operacional acessível deverá ser o de Desenvolvimento, com restrição total para uso dos demais ambientes (Homologação e Produção).

- Caso o prestador utilize softwares próprios em equipamentos da organização, deve-se apresentar documentação ou termo de responsabilidade garantindo direito de uso, que será mantido enquanto o software estiver instalado.

e) **Segurança física de microcomputadores**

- Este item se destina aos usuários e administradores de microcomputadores conectados ou não a uma rede;
- O objetivo é garantir que se estabeleça, administre e utilize microcomputadores de maneira segura, e que sejam tomadas medidas adequadas para respeitar a confidencialidade, integridade e disponibilidade das informações que são armazenadas e manipuladas através desses equipamentos.

e 1) Normas para segurança física de microcomputadores*:*

- Os meios de armazenamento digital devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas;
- Os microcomputadores não ligados a uma rede que contenham informações importantes para os negócios da empresa, devem estar instalados em uma estrutura que garanta a segurança física destes equipamentos, incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados;
- Os usuários ligados a uma rede e que manipulem informações importantes para os negócios da empresa, devem manter estas informações armazenadas nos servidores de rede.

e 2) Padrões para instalação de microcomputadores

- O padrão de instalação para os microcomputadores deve atender a todas as normas estipuladas pela ORION;
- A estrutura para manter a segurança física deve obedecer aos padrões de segurança geral da ORION e adequar-se às seguintes especificações:

- Sala:
  - ✓ As dimensões do local devem ser suficientes para a instalação dos equipamentos;
  - ✓ A disposição dos cabos lógicos e de energia devem ser adequadas de forma que as pessoas possam transitar livremente;
  - ✓ As entradas de ar (ventilação) dos equipamentos não devem estar obstruídas;
  - ✓ Os microcomputadores devem estar em locais firmes que evitem trepidações.

- Refrigeração e qualidade do ar:
  - ✓ Climatização deve ser conforme especificado pelo fabricante;
  - ✓ O ambiente deve estar livre de poluição por poeira, gases ou fumaça a fim de evitar que a poluição penetre nos equipamentos, possibilitando a quebra dos mesmos ou erros de processamento.

- Rede elétrica:
  - ✓ É recomendável que exista aterramento exclusivo para os equipamentos e que os pontos de energia sejam estabilizados;
  - ✓ Para os equipamentos considerados críticos recomenda-se a instalação de UPS (*Uninterruptable Power Supply)*, fonte alternativa de alimentação de energia que é ativada automaticamente quando ocorre a queda na alimentação de energia.
  - ✓ Os equipamentos devem ser instalados em uma rede elétrica seguindo os padrões recomendados pelos fabricantes;
  - ✓ As instalações elétricas devem sofrer revisões periódicas.

- Equipamentos Contra Incêndio:
  - ✓ Devem existir equipamentos de combate a incêndios adequados para materiais eletrônicos, tais como extintores de CO2, e estes devem estar em local visível sinalizado e desobstruído, e ser de conhecimento de todos os funcionários;
  - ✓ Devem existir equipamentos de prevenção de incêndios adequados, tais como detectores de fumaça e alarme contra incêndio, devendo existir um meio eficiente de aviso a um órgão de combate a incêndio. No caso das salas de servidores e/ou telecomunicações deve-se considerar o uso de dispositivos automatizados de combate à incêndios, gases do tipo FM 200 e outros recursos específicos à este tipo de ambiente

- Iluminação:
  - ✓ A iluminação deve ser adequada, evitando a incidência direta da luz do sol sobre os equipamentos.

- Precauções quanto à disponibilização dos meios de armazenamento:
  - ✓ Quando os meios magnéticos de armazenamento forem vendidos, devolvidos ao fabricante ou enviados para manutenção as informações neles contidas devem ser destruídas antes de deixar as dependências da ORION. Importante ressaltar que nos meios magnéticos não é suficiente apagar os dados, devendo-se executar um programa que realmente os destrua.

f) **Segurança física dos servidores de rede**

- Este item se destina aos usuários e administradores dos sistemas operacionais que necessitem de uma máquina com características de segurança de um servidor de rede;

- O objetivo é garantir que a ORION administre e utilize os diversos sistemas operacionais de maneira segura, e que sejam tomadas medidas adequadas para garantir a confidencialidade de seus dados, a integridade e disponibilidade dos equipamentos e meios de armazenamento.

f1) Normas para segurança física dos servidores de rede:

- Os meios de armazenamento devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas;
- Os servidores de arquivos devem estar instalados em uma área que garanta a segurança física destes equipamentos incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

f2) Padrões para instalação dos servidores de rede

- O padrão de instalação para servidores de rede deve atender a todas as normas estipuladas pela ORION;
- A estrutura para manter a segurança física dos equipamentos de uma rede deverá adequar-se às seguintes especificações:

  - Sala:
    - ✓ Fechada, mas permitindo a visualização interna do ambiente, com divisórias até o teto;
    - ✓ As dimensões do local devem ser suficientes para a instalação dos equipamentos;
    - ✓ A disposição dos cabos lógicos e de energia devem ser adequadas de forma que as pessoas possam transitar livremente;
    - ✓ As entradas de ar (ventilação) dos equipamentos não devem estar obstruídas;
    - ✓ Os servidores de rede devem estar em locais firmes que evitem trepidações.

  - Refrigeração e qualidade do ar:
    - ✓ Climatização adequada conforme especificado pelo fabricante;
    - ✓ O ambiente deve estar livre de poluição por poeira, gases ou fumaça a fim de evitar que a poluição penetre nos equipamentos, possibilitando a quebra dos mesmos ou erros de processamento.

- Rede elétrica:
  - ✓ Nos servidores, fazer uso de equipamento UPS (homologado por técnicos autorizados) com ”No Break”;
  - ✓ É necessário que exista aterramento exclusivo para os equipamentos e estabilização dos pontos de energia elétrica;
  - ✓ Os equipamentos devem ser instalados em uma rede elétrica exclusiva seguindo os padrões recomendados pelos fabricantes;
  - ✓ As instalações elétricas devem sofrer revisões periódicas.

- Equipamentos Contra Incêndio:
  - ✓ Devem existir equipamentos de combate a incêndio adequados para materiais eletrônicos, tais como extintores de CO2, e estes devem estar em local visível sinalizado e desobstruído, e ser de conhecimento de todos os funcionários;
  - ✓ Devem existir equipamentos de prevenção de incêndio adequados, tais como detectores de fumaça e alarme contra incêndio, devendo existir um meio eficiente de aviso a um órgão de combate a incêndio.

- Iluminação:
  - ✓ A iluminação deve ser adequada, evitando a incidência direta da luz do sol sobre os equipamentos.

- Precauções quanto à disponibilização dos meios de armazenamento:
  - ✓ Quando os meios magnéticos de armazenamento forem vendidos, devolvidos ao fabricante ou enviados para manutenção, as informações neles contidas deverão ser destruídas antes de deixar as dependências da ORION. Importante ressaltar que nos meios magnéticos não é suficiente apagar os dados, devendo-se executar um programa que realmente os destrua.
  - ✓ As manutenções dos meios magnéticos realizadas no próprio local, devem ser acompanhadas pelo responsável da área.

g) **Backup/Restore**

- Este item se destina aos usuários e administradores locais da ORION, visando administrar e utilizar os recursos de informática de maneira segura, tomando medidas adequadas que garantam recursos alternativos de processamento na eventualidade de perda dos dados, softwares ou sistemas.

- Para a elaboração de um plano de backup devem ser considerados os “backups” do tipo Operacional, Contingencial e Histórico.

- Backup Operacional é a cópia das informações estratégicas que fazem parte do quotidiano do usuário e que são importantes para garantir a continuidade de suas tarefas. Destina-se a recuperação instantânea;
- Backup Contingencial é a cópia das informações sensíveis, softwares e sistemas vitais à continuidade dos negócios da ORION e deve ser guardado em local externo. Destina-se a permitir a recuperação em situações catastróficas;
- Backup Histórico é a cópia das informações determinadas por exigência legal ou normas internas e deve ser guardado em local externo.

g 1) Normas para Backup / Restore:

- A elaboração do plano de backup/restore deverá levar em consideração os aspectos abaixo:
  - ✓ Os períodos de atualização dos dados;
  - ✓ Particularidades da atuação da ORION.
- As informações consideradas imprescindíveis devem estar presentes nas rotinas de backups operacional e contingencial, levando-se em consideração a periodicidade de atualização dos dados;
- As informações devem estar sujeitas às rotinas de backups operacional e contingencial conforme critério definido pela Diretoria Administrativa;
- As cópias de backup devem estar guardadas em local apropriado e seguro, e protegidas contra o acesso por pessoas não autorizadas;
- Deve-se manter uma cópia do plano de Backup/Restore juntamente com o backup contingencial;
- Devem ser realizados testes de restore periodicamente, mantendo evidências do último teste realizado;
- Devem ser mantidas, no mínimo, as duas últimas versões dos backups operacional e contingencial;
- Para os backups históricos, a quantidade de versões será determinada por exigência legal ou norma interna.

g 2) Responsabilidades Quanto a Backup / Restore:

- É de responsabilidade da área técnica da ORION, elaborar, manter e documentar o plano de backup e garantir a execução de seus procedimentos.

g 3) Plano de Backup / Restore - Conteúdo:

- Abrangência - Relação dos arquivos e diretórios a serem copiados no processo de backup;
- Periodicidade - Intervalo de tempo após o qual o sistema é submetido a rotina de backup;
- Retenção - Prazo pelo qual os backups devem ser mantidos;
- Procedimentos - Descrição dos procedimentos de backup;
- Quantidade de cópias - Número de cópias de backup, locais e meios de armazenamento;
- Identificação dos meios de armazenamento - Os meios de armazenamento devem estar devidamente identificados;
- Registro do uso das cópias de backup - A manipulação dos meios de armazenamento deve ser registrada e controlada. Estes registros devem ser guardados por 90 (noventa) dias para futuras verificações;
- Manutenção das cópias Backup - Quand dados em novo meio periodicamente.

h) **Responsabilidades quanto ao Backup/Restore**

- É de responsabilidade área técnica da ORION elaborar, manter e documentar o plano de backups e garantir a execução de seus procedimentos.
- O plano deve conter:
  - **Abrangência** – Relação dos arquivos e diretórios a serem copiados no processo de backup;
  - **Periodicidade** - Intervalo de tempo ao qual o sistema é submetido a rotina de backup;
  - **Retenção** - Prazo pelo qual os backups devem ser mantidos;
  - **Procedimentos** - Descrição dos procedimentos de backup;
  - **Quantidade de cópias** - Número de cópias de backup, locais e meios de armazenamento;
  - **Identificação dos meios de armazenamento** - Os meios de armazenamento devem estar devidamente identificados;
  - **Registro do uso das cópias de backup** - A manipulação dos meios de armazenamento deve ser registrada e controlada. Estes registros devem ser guardados por 90 (noventa) dias para futuras verificações;
  - **Manutenção das Cópias Backup** - Quando o prazo de retenção for superior ao especificado pelo fabricante para utilização do meio de armazenamento, deve-se adotar um procedimento para regravação dos dados, em novo meio, periodicamente.

i) **Testes regulares**

- Todo e qualquer meio de armazenamento assim como os procedimentos de recuperação devem ser regularmente testados, garantindo sua efetividade. A periodicidade deve ao menos ser uma por ano, a ser determinada pelo Comitê de Segurança e Contingência, considerando o nível de risco do negócio.
- Deve-se manter evidências do sucesso dos testes feitos.

j) **Pirataria**

- Este item se destina a todos os usuários e administradores de servidores de redes ou microcomputadores, inclusive portáteis, conectados ou não a uma rede e tem como objetivo garantir que sejam tomadas medidas adequadas para coibir a pirataria de softwares dentro das instalações da ORION.

j 1) Normas contra pirataria:

- A quantidade de licenças de softwares não pode ser inferior à quantidade de softwares instalados, mesmo que para fins de testes ou treinamentos, a não ser que esta situação esteja coberta contratualmente;
- Não é permitido duplicar software de propriedade da ORION a não ser com a finalidade de cópia de segurança e mesmo assim, somente por pessoas autorizadas;
- Uma licença de uso de software da ORION só pode ser instalada em micros particulares caso esta licença não esteja instalada em um dos equipamentos da ORION e se tiver autorização do responsável administrativo direto pelo usuário;
- Não é permitido executar ou instalar qualquer software (inclusive software livre e de domínio publico), telas de "screen saver", “papéis de parede”, etc., que não estejam autorizados pela Diretoria Administrativa.
- Todo software de demonstração deve vir acompanhado de nota fiscal ou carta da empresa proprietária, formalizando onde pode ser instalado e por quanto tempo;
- A utilização de software do tipo “shareware” só deve ser feita após a obtenção do registro junto ao autor e após homologação da área técnica da ORION.
- É proibida a utilização e reprodução não autorizada de manuais, livros, revistas, periódicos protegidos por direitos autorais.

j 2) Responsabilidades quanto a pirataria:

- É da responsabilidade área técnica da ORION:
  - ✓ Verificar se o software a ser instalado é original, conferindo o mesmo com as devidas licenças de uso;
  - ✓ Se a instalação foi autorizada pelo responsável administrativo direto pelo usuário, somente se homologado anteriormente pela Metro Tecnologia & Sistemas;
  - ✓ Implementar mecanismos que dificultem a pirataria através de qualquer meio.

k) **Utilização segura de hardware e software**

- Todos os equipamentos portáteis (notebooks, laptops, etc.) que tenham capacidade de armazenamento de dados, devem ser protegidos conforme especificação da ORION. Quando estes equipamentos contiverem informações que não possam ser de conhecimento público, as mesmas devem ser criptografadas ou ter seu acesso protegido por senha;
- É proibida a utilização de hardware ou software particulares nas dependências das Empresas da ORION, exceto em casos especiais de extrema necessidade e com prévia autorização do Diretor Administrativo.
- É expressamente vedada a aquisição, reprodução, utilização e cessão de cópias não autorizadas de “softwares” ou de quaisquer programas e produtos, mesmo aqueles desenvolvidos pelas áreas técnicas da ORION ou desenvolvidos por terceiros para a ORION;

l) **Acesso à Internet**

- Internet abrange vários aspectos e serviços (“sites” de serviço governamentais, prestadores de serviço, etc) que devem ser disponibilizados ou controlados conforme as necessidades de negócio. A restrição a “sites” não relativos aos negócios da organização deve ser implementada, garantindo o uso efetivo da rede Internet.
- O acesso à Internet deve ser feito através de “Servidores de Acesso” protegidos por sistemas de “Firewall”. Quando for necessário o acesso utilizando “Modens locais“ a configuração da máquina deve garantir o isolamento da rede normal de serviço da empresa, evitando assim que uma contaminação seja propagada. Os requisitos de segurança destas máquinas em particular devem ser respeitadas (anti-virus, firewall local). Casos específicos como esses devem ser aprovados pelos responsáveis da área de Produção e Suporte.
- Todos os colaboradores são orientados a não acessar sites e/ou conteúdos que não sejam relacionados às suas atividades dentro da empresa. Desde o processo de

contratação, on-boarding e nas sessões de boas práticas de segurança da informação, os colaboradores recebem orientações quanto a acesso a sites e conteúdos indevidos.

m) **Acesso ao Correio Eletrônico**

- A ORION disponibiliza aos seus funcionários a tecnologia necessária a fim de facilitar a comunicação interna, comunicação com clientes, fornecedores e outros grupos que tenham relação comercial com a mesma. É de responsabilidade do usuário a utilização da tecnologia de forma adequada, prudente, e de modo compatível com as leis e princípios aplicáveis aos negócios.
- Por consequência, devem ser observadas as orientações descritas nos itens a seguir.

m 1) Aspectos Gerais

- Utilizar o sistema de correio eletrônico apenas para fins profissionais compatíveis com as funções exercidas.
- Não fornecer o endereço de correio eletrônico profissional ou da empresa, em situações de caráter pessoal.
- Usar linguagem apropriada, não utilizando termos vulgares.
- O correio eletrônico não pode – e não deve – substituir completamente a interação pessoal.
- Lembrar que, ao ser utilizado o correio eletrônico para comunicação com clientes ou parceiros de negócio, devem ser seguidos os mesmos princípios, e tomados os mesmos cuidados, aplicáveis a toda e qualquer forma de comunicação externa.
- É recomendado que os endereços de correio eletrônico da empresa estejam localizados num domínio que se refira claramente ao nome da empresa (por ex. atendimento@*ORION*.com.br.
- Caso a empresa se utilize de caixas postais para contato com o público em geral, cujos endereços sejam exibidos em páginas da Internet, devem ser utilizadas caixas postais departamentais.
- No cartão de visitas empresarial deve sempre constar o endereço da caixa postal profissional, departamental, ou individual quando existir. Nunca deverá constar a caixa postal particular do funcionário.

m 2) Aspectos Legais

- Caso seja evidenciada a má utilização do sistema de correio eletrônico, a empresa poderá aplicar penalidades cabíveis, incluindo o término do contrato de trabalho do

responsável pela ação. Considera-se má utilização do sistema de correio eletrônico o envio ou encaminhamento de mensagem contendo, entre outras coisas:

- ✓ Informações de negócio da empresa sem autorização adequada;
- ✓ Material que possa infringir direitos autorais ou outros direitos de propriedade intelectual;
- ✓ Informação comercialmente delicada ou contenciosa, isto é, aquela que possa gerar algum tipo de discussão judicial, ou que possa ter implicações legais ou contratuais para a empresa, a menos que tenha um objetivo de negócio específico e autorizado;
- ✓ Texto que possa causar responsabilidades cíveis, comerciais, criminais, ou outras;
- ✓ Apologia ou incentivo à violência, desobediência civil ou a atitudes e atos ilegais;
- ✓ Informação que possa prejudicar a reputação da empresa ou o relacionamento com seus parceiros de negócios, ou que possa constrangê-los;
- ✓ Material pornográfico, ou qualquer outro material de cunho semelhante;
- ✓ Texto que possa ser classificado como discriminação sexual, racial ou de qualquer outra natureza;
- ✓ Material vulgar, com piadas, ou descrevendo situações humilhantes, preconceituosas ou constrangedoras;
- ✓ Texto que possa ser considerado como uma ameaça;
- ✓ Texto formando ou participando de uma “corrente”;
- ✓ Texto com fins políticos ou religiosos;
- ✓ Material para atividades comerciais particulares ou propagandas não oficiais.
- ✓ Não devem ser respondidas ou encaminhadas mensagens com teores impróprios, conforme citado no ítem anterior. Se forem recebidas mensagens desta natureza, deverão ser imediatamente eliminadas.

m 3) Aspectos Operacionais

- Ler a caixa de entrada regularmente, de preferência, pelo menos duas vezes ao dia.
- Caso a empresa possua serviços de atendimento a clientes através de correio eletrônico, as mensagens recebidas devem ser respondidas no prazo máximo de 48 horas;
- Em caso de ausência, é recomendável que seja utilizada uma das seguintes opções:
  - ✓ Acesso remoto à caixa postal, através do software Webmail,;
  - ✓ Redirecionamento da caixa postal para a de outro funcionário;
  - ✓ Resposta automática, mencionando o período de ausência e sugerindo alternativas para encaminhamento da mensagem;

- Utilizar pastas classificadas por assunto, caso seja necessário guardar as mensagens recebidas ou enviadas, de forma a manter as caixas de entrada e de saída com um mínimo de mensagens. Isso facilitará a administração das mensagens recebidas e enviadas.
- Não anexar arquivos contendo textos ou informações que poderiam estar no corpo da mensagem. Dessa forma, o destinatário não terá que abrir o arquivo anexo para ler o seu conteúdo.
- Anexar arquivos a mensagens é útil, se o arquivo contém alguma formatação relevante ou alguma informação em formato que não seja texto, por exemplo, planilhas ou gráficos. Deve ser evitada a anexação de arquivos com tamanho superior a 15 (quinze) megabytes.
- É interessante que conste no rodapé do arquivo anexado, o e-mail do remetente, análogo ao endereço do remetente em correspondências convencionais.
- Caso a resposta a uma mensagem não tenha retornado dentro do prazo esperado, não deve ser assumido que a mesma foi ignorada. Verificar, polidamente, se a mensagem foi recebida. É responsabilidade de quem envia verificar se o destinatário recebeu a mensagem, e cortesia do destinatário informar sobre o recebimento da mesma.

m 4) Aspectos de Segurança

- Lembrar que o correio eletrônico não garante privacidade, isto é, transmissões via Internet podem ser interceptadas por outros, ou ser alteradas antes de chegar ao destinatário.
- Para garantir a privacidade de uma mensagem, a mesma deverá ser criptografada.
- Não abrir arquivos anexos os quais não tenham sido solicitados;
- **N**ão clicar em "links", ou abrir arquivos anexos, cuja extensão seja ".exe", ".pif" ou ".com";
- Não clicar em "links" cujo endereço da página não corresponda ao endereço (@domínio) do remetente;

m 5) Aspectos Técnicos

- Não enviar mensagens com arquivos grandes anexados. Arquivos maiores poderão ser compactados, ou encaminhados aos destinatários por outros meios. Devem ser utilizados somente utilitários homologados e legalizados.
- Quando forem enviadas mensagens com arquivos anexados, é importante certificar-se que o destinatário possui um software adequado para abri-los.

- Eventualmente o sistema de correio de eletrônico poderá enviar uma notificação informando que uma mensagem não pode ser entregue. Quando isso ocorrer deve-se:
  - ✓ Verificar se o endereço do destinatário está correto. Caso haja algum erro, corrigir e reenviar a mensagem;
  - ✓ Verificar se outras pessoas, também estão tendo problemas com o correio eletrônico. Em caso afirmativo, aguardar e tentar reenviar a mensagem mais tarde.

n) **Plano de Conscientização de Segurança da Informação**

- Um plano de conscientização da segurança da informação deve ser elaborado e executado para atingir os seguintes objetivos:
- Garantir que a Segurança da Informação não seja apenas conhecida, mas compreendida por todos os funcionários e colaboradores, conscientizando-os sobre melhores práticas, requisitos mínimos, riscos e responsabilidades existentes e quais medidas devem ser adotadas quando ocorrerem incidentes de Segurança de forma a atingir uma melhor utilização e proteção à informação.

n1) As diretrizes básicas são:

- ✓ Elaboração de um processo de treinamento continuado contemplando todos os níveis funcionais da *ORION*;
- ✓ Divulgação de diversos materiais e alertas pela Intranet referente a Segurança da Informação para funcionários, colaboradores e clientes;
- ✓ Organização de eventos que tenham o intuito de fortalecer a conscientização sobre diversos aspectos de segurança em geral;
- ✓ Revisão periódica do plano, adequando as ações às novas necessidades, evitando torná-lo repetitivo.

o) **Ambientes CLOUD (SaaS)**

- Apenas a área de TI da ORION terá acesso a infraestrutura e serviços da rede Orion AWS;
- Todo e qualquer acesso aos servidores e recursos (*fileshare* e banco de dados), onde se encontram dados de clientes, que se faça necessário para eventual manutenção deverá passar pelo processo de notificação e autorização dos responsáveis envolvidos ao ambiente (cliente e Orion);
- Usuários ORION, com exceção ao time de TI, não terão acesso aos sistemas e recursos (servidores, *fileshare* e banco de dados) de clientes. Caso haja alguma necessidade

específica, o gestor da área deverá solicitar ao cliente devida permissão e acompanhamento para acesso;

- Usuários ORION não poderão acessar ou visualizar qualquer ativo de informação de clientes sem a devida autorização e acompanhamento;
- Ambientes produtivos devem ser separados e apartados do ambiente de testes e homologação disponibilizados aos clientes. Esta separação deve ser física onde servidores, banco de dados e outros recursos necessários devem ser distintos para cada ambiente;
- Dados de ambientes produtivos NÃO podem ser movidos ou copiados para outros ambientes, com exceção para casos de ambientes de DR (Disaster Recovery);
- Dados de ambientes de teste ou homologação devem ser mascarados para devida proteção e confidencialidade, mas serão de responsabilidade do cliente realizar tal procedimento;

p) **Descarte de dados contidos em mídias de armazenamento digital**

- A área de TI da ORION será responsável pelo descarte de dados e mídias digitais inutilizadas;
- Dados contidos em mídias de armazenamento digital como CDs, DVDs, pen drives, cartões de memórias, SSD e HDs deverão ser apagadas com o uso de softwares para apagamento seguro de dados
- Para a eliminação de dados a partir de mídias do tipo HD poderão ser utilizados desmagnetizadores.
- Para a eliminação de dados a partir de mídias como SSD, o processo deverá ser realizado quantas vezes forem necessárias para diminuir o máximo da permanência de dados da mídia.
- Mídias de armazenamento digital deverão ser inutilizados somente após a inutilização dos dados contidos. Deverão ser destruídos fisicamente, e caso isso não seja possível, deverá ser encaminhado para descarte por uma entidade credenciada pela Orion.
- Não é permitido o reuso de qualquer tipo de mídia digital fora do contexto corporativo e que seja identificado, autorizado e disponibilizado pela Orion TI.

q) **Papéis e Responsabilidades**

- A revisão e atualização anual dessa Política é de responsabilidade da Área de TIC, Departamento de Segurança da Informação.

- A sessões de divulgação de informaçoões, boas práticas e treinamentos sobre Segurança da Informação são realizadas em parceria entre o Departamento de Segurança da Informação e a Área de Compliance.
- A aplicação de controles, rotinas, procedimentos relacionados a Segurança da Informação e acessos físicos e lógicos são de responsabildade da Área de TIC.
- Todos os líderes de área são responsáveis por zelar pelo cumprimento da Política de Segurança da Informação perante suas equipes e devem notificar o Departamento de Segurança da Informação em caso de violações, brechas ou qualquer evento relacionado a acessos indevidos, sejam físicos ou lógicos.
- Todos os Colaboradores são reponsáveis por seguir as determinações e práticas estabelecidas na Política de Segurança da Informação.

r) **Segregação de Ambientes**

r1) Princípios Gerais

- ***Separação física ou lógica**: Cada ambiente deve ser isolado, seja por infraestrutura (servidores distintos) ou por mecanismos de virtualização/containerização.*
- ***Controle de acesso**: Definir perfis e permissões específicas para cada ambiente, garantindo que apenas usuários autorizados possam realizar operações.*
- ***Consistência de configuração**: Manter configurações alinhadas entre ambientes, evitando divergências.*

r2) Ambientes de Desenvolvimento

***Objetivo**: Permitir que desenvolvedores criem, testem e validem funcionalidades.*

***Boas práticas**:*

- *Liberdade para testes, mas com monitoramento básico para evitar impactos.*
- *Integração contínua (CI) para validar código antes de seguir para homologação.*

r3) Ambientes de Homologação

***Objetivo**: Validar funcionalidades com dados próximos ao real, garantindo qualidade antes da produção.*

***Boas práticas**:*

- *Testes funcionais, de carga e segurança.*
- *Acesso restrito a equipe de QA e stakeholders autorizados.*

Deploy automatizado a partir do repositório oficial (sem alterações manuais).

r4) Ambientes de Produção

***Objetivo**: Executar o sistema em condições reais para usuários finais.*

***Boas práticas**:*

- *Proibição de testes: Nenhum teste deve ser realizado diretamente em produção.*
- *Controle rigoroso de acesso: Apenas equipe de operação e suporte autorizado.*
- *Monitoramento contínuo: Logs, métricas e alertas para garantir disponibilidade e segurança.*
- *Plano de rollback: Sempre ter estratégia para reversão segura em caso de falhas.*

r5) Segurança

- *Segregação de credenciais: Cada ambiente deve ter credenciais distintas.*
- *Política de backups: Frequência definida e testes de restauração.*

s) Procedimentos de “Mesa Limpa” e Acesso à Sala ADM/FIN

S1) Princípios Gerais

As mesas dos colaboradores não possuem gavetas e/ou armários individuais. Todos os itens pessoais são armazenados em local separado, em armários com chave.
Documentos corporativos, quando físicos (impressos) são armazenados na sala Administrativo/Financeiro e RH em armários com chave. O acesso a essa sala e feito por controle biométrico com reconhecimento facial, sendo que somente os times Administrativo/Financeiro e RH, e seus respectivos diretores, possuem acesso ao local.

S2) Procedimentos de Mesa Limpa

Com o objetivo de garantir a proteção das informações corporativas, evitar acessos não autorizados e promover um ambiente de trabalho organizado e seguro, todos os colaboradores

devem assegurar que, ao se ausentarem de suas estações de trabalho – mesmo que temporariamente –, nenhuma informação sensível ou documento corporativo permaneça exposto. Isso inclui papéis, anotações, dispositivos eletrônicos, mídias removíveis e quaisquer materiais que possam conter dados confidenciais.

Ao final do expediente, as mesas devem permanecer livres de documentos físicos, cadernos, equipamentos não essenciais e materiais que contenham informações estratégicas ou pessoais. Todos esses itens devem ser devidamente guardados em armários, gavetas ou outros locais protegidos.

Em alinhamento com essa prática, a sala administrativa onde são armazenados documentos físicos permanece trancada diariamente e conta com dispositivo de reconhecimento facial, garantindo que apenas pessoas autorizadas possuam acesso ao local.

4. Glossário

Termo	Descrição
TIC	Área de TI e Comunicações
No Break	Equipamento para manutenção da rede elétrica em caso de falhas elétricas ou falta de energia
Backup	Cópia de segurança para dados e informações em formato digital
Restore	Procedimento de recuperação de uma cópia de segurança

5. ANEXOS

a 1) Modelo de Termo de Responsabilidade*:*

Eu (Nome do Funcionário), código funcional Nº (número), CPF Nº (número) declaro para os devidos fins e efeitos de direito que a(o) (Nome da Empresa) trouxe ao meu conhecimento o conteúdo das diretrizes, violações, normas e responsabilidades que regem sua Política de Segurança de Informação, que ora declaro ter lido, estando ciente e responsável pelo que segue :

1. Qualquer meio de acesso às informações ou instalações (como identificações de usuário, senhas, crachás, cartões, chaves, etc.) que a empresa me forneceu ou vier a fornecer são pessoais, intransferíveis, estarão sob minha custódia e serão utilizados exclusivamente no cumprimento de minhas responsabilidades perante a ORION, devendo ser por mim devolvidos em caso de desligamento;
2. Todas as informações utilizadas na ORION, sejam elas de sua propriedade ou de terceiros, possuem caráter confidencial e sigiloso, motivo pelo qual comprometo-me a manuseá-las de maneira segura e somente no exercício de minhas atividades, evitando sua perda, furto, cópia, utilização indevida ou divulgação não autorizada;
3. A ORION está autorizada a consultar e analisar informações registradas em qualquer meio localizado em suas instalações e que tenham sido geradas ou recebidas utilizando seus recursos, inclusive correspondências recebidas em nome ou endereço da mesma;
4. Não devo adquirir, reproduzir, utilizar ou distribuir cópias não autorizadas ou legalmente adquiridas de "softwares" ou programas produtos, mesmo aqueles desenvolvidos internamente pelas áreas técnicas da ORION;
5. Devo zelar pela segurança, uso correto e manutenção adequada dos equipamentos existentes na ORION;
6. As informações por mim geradas ou recebidas durante minha jornada de trabalho deverão tratar apenas de assuntos profissionais e ligados exclusivamente ao exercício de minha função;
7. Descumprindo os compromissos por mim assumidos nesta declaração estarei sujeito as penalidades aplicáveis, como medidas administrativas/disciplinares internas e/ou ações penais/cíveis previstas em lei.

.....(Cidade e Data).....

.....(Assinatura do Funcionário)...

a 2) Modelo de Termo de Responsabilidade para Empresas Contratadas*:*

As empresas prestadoras de serviço devem ser orientadas para que mantenham documento similar em seus arquivos, assinado pelos funcionários por ela contratados para prestar serviços na ORION, devendo o texto abaixo ser incluído nos contratos de prestação de serviço:

"Fica a Contratada, responsável pela orientação dos funcionários por ela indicados para trabalharem junto à contratante, no que diz respeito ao cumprimento das Políticas de Segurança da Informação da Contratante, cumprimento das Leis de Copyright e de Combate a Pirataria de Softwares.

Fica também a Contratada co-responsável pela utilização das senhas e uso das informações por parte dos funcionários por ela contratados e disponibilizados para atuação junto a Contratante, de acordo com o termo de responsabilidade assinado pelo funcionário da Contratada. Esta co-responsabilidade estende-se inclusive aos foros judiciais, sob todos os aspectos, inclusive o do direito das obrigações.".