Área Responsável	Título	Classificação	Versão	Emissão / Vencimento	Página
SEGURANÇA DA INFORMAÇÃO	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DE TERCEIROS**	**PÚBLICA**	**03**	**25/02/2025** Vencimento **25/02/2026**	**1/13**

OBJETIVO DA POLÍTICA

Estabelecer os requisitos mínimos de Segurança da Informação e privacidade para os terceiros que têm acesso aos dados/informações da Orizon em suas diversas formas, conforme os requisitos do negócio, com as leis e regulamentações pertinentes, primando pela confidencialidade, integridade, disponibilidade e autenticidade.

ABRANGÊNCIA

Aplica-se, independentemente de suas atribuições e responsabilidades, a todos os colaboradores da Companhia Brasileira de Gestão de Serviços (“CBGS”) e suas afiliadas, bem como a todos visitantes, terceiros, prestadores de serviço e partes interessadas em suas relações conosco, assim entendidas as empresas por ela controladas, sob controle comum e/ou coligadas, doravante denominadas em conjunto simplesmente como “Orizon”.

COMO ERA?

PÁGINA	COPIAR AS CLÁUSULAS PRINCIPAIS QUE SERÃO ATUALIZADAS
Cabeçalho	Classificação anterior: INTERNA

O QUE MUDOU?

PÁGINA	COPIAR AS CLÁUSULAS PRINCIPAIS JÁ ALTERADAS
Cabeçalho	Classificação atualizada para: PÚBLICA

INDICE

- ABRANGÊNCIA 1
- COMO ERA? 1
- O QUE MUDOU? 1

1. DOCUMENTAÇÕES COMPLEMENTARES 3
2. CONCEITOS E SIGLAS 3
3. DISPOSIÇÕES GERAIS 4
4. DIRETRIZES 4
5. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO 5
6. NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 6
7. CONTROLES DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DE TERCEIROS 6

7.1. Privacidade 6
7.2. Gestão de Vulnerabilidades 7
7.3. Configurações Seguras (Hardening) 7
7.4. Controle de Acessos 7
7.5. Monitoramento dos Serviços e Gestão de Incidentes 7

8. SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS 7
9. CLASSIFICAÇÃO DA INFORMAÇÃO 8
10. MANIPULAÇÃO DAS INFORMAÇÕES 8
11. SEGURANÇA FÍSICA 8

11.1. Escritórios 8
11.2. Câmeras de Segurança 9
11.3. Uso do Crachá 9
11.4. Estações de Trabalho 9
11.5. Monitoramento 9

12. SERVIÇOS E CERTIFICAÇÕES 9
13. CONTINUIDADE DE NEGOCIOS E GESTÃO DE BACKUPS 10
14. DA LEI GERAL DA PROTEÇÃO DE DADOS 10
15. RESPEITO À DIVERSIDADE, EQUIDADE E INCLUSÃO 11

1. DOCUMENTAÇÕES COMPLEMENTARES

Código de Confiança

Política Empresarial de Privacidade e Proteção de Dados

Política de Gestão de Riscos Corporativos

Política de Gestão de Continuidade de Negócios

Política de Consequências

Política de Resposta a Incidentes de Segurança da Informação e Segurança Cibernética

Norma de Controle de Acesso Físico

Norma de Gestão de Fornecedores

Norma de Utilização de Software

Norma de Classificação da Informação

Norma de Controle de Acesso aos Sistemas de Informação

Procedimento de Mesa e Tela limpa

Guia TISS vigente, disponível no site da Agência Nacional de Saúde (ANS)

2. CONCEITOS E SIGLAS

Ativo: Qualquer coisa, tangível ou intangível que tenha valor para a organização.

Ativos de Informação: É o recurso físico ou lógico utilizado no armazenamento e manuseio da informação, por exemplo: documentos em papel, computadores, base de dados.

Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

Continuidade de Negócios: Processo para garantir que os serviços essenciais da Orizon sejam devidamente identificados, priorizados e documentados, para manter a empresa operacional, com o menor impacto possível aos clientes, mesmo após um desastre, até o retorno à situação normal.

CSIRT (Computer Security Incident Response Team): Equipe de Resposta a Incidentes de Segurança de Computadores.

Disponibilidade: Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

Informação: É qualquer conteúdo ou dado que tenha valor para a organização.

Integridade: Propriedade de salvaguarda da exatidão e completeza de ativos.

SI: Segurança da Informação.

Segurança física: Trata-se da proteção do ambiente tangível, composta por equipamentos biométricos, câmeras e portas.

Segurança lógica: Trata-se da proteção do ambiente intangível, composta por softwares, sistemas ou aplicações.

TI: Tecnologia da Informação.

VPN (Virtual Private Network): Sigla que designa rede virtual privada.

3. DISPOSIÇÕES GERAIS

A Política de Segurança da Informação de Terceiros tem como objetivo estabelecer responsabilidades, princípios, diretrizes e orientações relacionada ao uso adequado de ativos e recursos tecnológicos pelos Terceiros na Orizon.

4. DIRETRIZES

Os terceiros, prestadores de serviço ou fornecedores, devem cumprir com todos os requisitos da legislação brasileira aplicáveis e comprometer-se integralmente com os itens:

- Terceiros devem passar por processo de avaliação de Segurança da Informação, através da Avaliação de Fornecedor de Segurança da Informação na fase de contratação;
- Garantir a preservação das informações Orizon contra danos, alterações, acesso ou divulgação não autorizados, assegurando sua confidencialidade;
- Assegurar que os sistemas e as informações sob sua supervisão estejam protegidos de maneira apropriada;
- Observar e cumprir integralmente as leis e regulamentos que regem os aspectos relacionados à propriedade intelectual;
- Selecionar os mecanismos de Segurança da Informação, considerando cuidadosamente as ameaças e riscos associados às suas atividades;

- Em caso de armazenamento e/ou processamento de dados pessoais de clientes, funcionários, financeiro ou prestação de serviço de nuvem para a Orizon, é necessário garantir que esteja em conformidade com os normativos e requisitos de Privacidade e Proteção de Dados bem como ao Código de Conduta e Confiança do Fornecedor da empresa;
- Garantir que os recursos fornecidos estejam sendo utilizados exclusivamente para as finalidades aprovados pela Orizon;
- Atender às leis que regulamentam as atividades da Orizon e seu mercado de atuação;
- Estar ciente de que Segurança da Informação da Orizon poderá efetuar avaliações e testes técnicos na infraestrutura do terceiro, mediante necessidade, para garantir a segurança e cumprimento das melhores práticas de mercado;

5. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

A. O terceiro deverá acessar os ambientes de infraestrutura Orizon somente através de VPN, que deverá ser devidamente segregada, das demais redes VPN para colaboradores Orizon;

B. O terceiro, com dispositivo próprio, não deve acessar os ambientes e recursos de infraestrutura Orizon sem a conexão de VPN, mesmo que presencialmente via cabo;

C. Os acessos lógicos ao ambiente ou recursos da rede interna da Orizon deverá ser solicitado pelo gestor responsável pela contratação. A solicitação será realizada por ferramenta de chamados, avaliada e aprovada conforme cada demanda, seguindo as diretrizes corporativas de Segurança da Informação;

D. A proteção dos dispositivos físicos de terceiros, contendo informações da Orizon, é de responsabilidade do usuário. Devendo aplicar e preservar controles de proteção acesso, criptografia de repouso ou trânsito (quando aplicável) e defesas contra ameaças cibernéticas, para salvaguardar essas informações;

E. Dentro da rede da Orizon, é estritamente proibido acessar, baixar ou distribuir qualquer conteúdo que viole direitos autorais ou de propriedade. Da mesma forma, não é permitido acessar ou distribuir conteúdo pornográfico.

F. Os dispositivos de terceiros não podem ser conectados nas redes de desenvolvimento, homologação ou produção da Orizon sem a aprovação direta de Segurança da Informação e ciência na declaração de anuência da Orizon para dispositivos particulares, sendo que estes deverão obrigatoriamente estar protegidos por softwares de segurança homologados por Segurança da Informação;

G. É proibido o compartilhamento de usuários e senhas entre os prestadores de serviços, o terceiro tem que manter suas credenciais de acesso seguras, sendo de sua responsabilidade qualquer utilização

indevida evitando escrevê-las e deixá-las com acesso facilitado, preferindo-se a memorização ou uso de cofres de senha.

H. Todos os terceiros são obrigados a realizar treinamentos de Segurança da Informação fornecidos pela Orizon durante o início da contratação por todos os meios disponíveis;

I. É responsabilidade da empresa terceira comunicar qualquer desligamento de seus colaboradores para que eles tenham seus acessos devidamente cancelados no ambiente da Orizon, prazo não posterior a 24 horas após o desligamento;

6. NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Qualquer incidente ou não conformidade de Segurança da Informação conhecido por um terceiro deve ser prontamente comunicado diretamente à Orizon ou ao responsável pelo contrato, para que este possa iniciar o processo de notificação de incidente através dos canais formais estabelecidos.

Os incidentes podem ser reportados para **cis@orizon.com.br** contendo a descrição do incidente identificado e se possíveis anexos como capturas de tela, por exemplo. Demais canais de comunicação podem ser encontrados na Política de Resposta a Incidentes de Segurança da Informação e Segurança Cibernética no item "**CANAIS DE ENTRADA DE POSSÍVEIS INCIDENTES"** que estará sempre atualizado com outros meios de contato.

7. CONTROLES DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DE TERCEIROS

7.1. Privacidade

A empresa terceira deverá seguir as melhores práticas de mercado voltadas a Privacidade e Proteção de dados pessoais, sendo legalmente obrigada a cumprir com os controles elencados na Lei 13.709/2018, seguindo a abordagem de Privacy and Security by Design e devendo possuir, mas não se limitando a:

A. Avaliação de impacto relacionada aos dados pessoais de um titular (DPIA) e um processo que garanta à Orizon acesso irrestrito às suas informações processadas e armazenadas, conforme definido no escopo do serviço prestado;

B. Notificar a Orizon sobre as informações coletadas, seu propósito, a base legal para o processamento dos dados, onde são armazenadas e por quanto tempo, além de procurar minimizá-las sempre que viável;

C. Fornecer documentação que detalhe o fluxo dos dados da Orizon no ambiente do fornecedor, abrangendo todo o seu ciclo de vida, desde a coleta até a exclusão, incluindo processamento, armazenamento e compartilhamento.

7.2. Gestão de Vulnerabilidades

O terceiro se compromete junto a Orizon a desenvolver e seguir um fluxo definido de gestão de vulnerabilidades que garanta a prevenção, detecção e correção de vulnerabilidades, abrangendo aspectos como realização regular de testes e varreduras e aplicação regular de patches de atualização de segurança.

O terceiro também se compromete no cumprimento dos prazos do normativo Orizon **"Norma de Gerenciamento de Vulnerabilidades"** relacionado a aplicação de correções de vulnerabilidades críticas e altas identificadas em seus sistemas, devendo solicitar as informações sempre que necessário.

7.3. Configurações Seguras (Hardening)

O terceiro deverá minimamente realizar a aplicação de hardening em seus servidores e estações de trabalho atingindo no mínimo o Grupo de Implementação L1 do CIS Controls para sistemas operacionais e aplicações que de alguma forma forneçam ou sustentem serviços para a Orizon.

7.4. Controle de Acessos

A empresa parceira deverá possuir processo formalizado de concessão, alteração e revogação de acessos, principalmente aqueles com acessos privilegiados, documentando o processo de Gerenciamento de Acessos baseados em práticas de RBAC.

7.5. Monitoramento dos Serviços e Gestão de Incidentes

O terceiro deve identificar e registrar incidentes relacionados à Segurança da Informação em seu ambiente e notificar a Orizon sobre incidentes que tenham a possibilidade de gerar impacto a organização, como acessos não autorizados, perda de dados, comprometimento de sistemas, entre outros tipos de incidentes de segurança classificados pelo NIST SP 800-61 Incident Handling.

8. SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS

Para terceiros que possuem atividades relacionadas ao desenvolvimento de sistemas, deverá ser incluídas verificações de segurança no processo de desenvolvimento como revisão de código utilizando tecnologia específica

SAST e/ou DAST, testes de intrusão periódicos, contemplando pelo menos as que estão listadas no OWASP ASVS, OASP testing guide e OWASP SAMM.

9. CLASSIFICAÇÃO DA INFORMAÇÃO

O terceiro se compromete em utilizar e respeitar a classificação de informação mediante a relevância da informação ou dado, se atentando aos aspectos de manuseio através da rotulagem, armazenamento, transporte e descarte da informação.

Neste contexto é importante ter ciência que documentos como contratos, registros financeiros, comerciais, relatórios internos de qualquer natureza, planos e projetos, entre outros, contém informações que são de propriedade da Orizon.

Documentos produzidos pela e para a Orizon não devem ser publicados, a não ser que devidamente autorizados para este fim.

A Norma de Classificação de Informação estabelece como as informações da Orizon são classificadas.

10. MANIPULAÇÃO DAS INFORMAÇÕES

Todas as informações da Orizon devem ser armazenadas na rede corporativa ou ambientes colaborativos em nuvem da própria Orizon (OneDrive e Sharepoint - Office 365), sendo vedado armazenar e transferir informações ou dados para dispositivos e ou meios de armazenamento externos, incluindo, mas não se limitando a: Unidades USB (Pendrivers, Flashdrivers etc.), HDs Externos, chats, Inteligências Artificiais e ambientes de armazenamento em nuvem e não homologados (Dropbox, OneDrive (de terceiros), iCloud, Google Drive etc.).

11. SEGURANÇA FÍSICA

11.1. Escritórios

Fica vedado fotografar ou filmar as instalações da Orizon, exceto o espaço reservado para conveniência, salvo por exceções previamente autorizadas. Todo e qualquer acesso é feito por portas com controle de acesso eletrônico. As portas de combate a incêndio devem ser mantidas fechadas, a abertura das portas de incêndio só pode ser realizada em emergência ou devidamente autorizada pela brigada de incêndio.

11.2. Câmeras de Segurança

Os ambientes da Orizon são monitorados por câmeras de segurança, e as gravações são ser armazenadas conforme diretrizes internas.

11.3. Uso do Crachá

O crachá é considerado um instrumento de Segurança da Informação e o uso nas dependências da Orizon é obrigatório, conforme regras estabelecidas na **"Norma de Controle de Acesso Físico"**.

11.4. Estações de Trabalho

Os laptops devem ser protegidos com criptografia de dados utilizando tecnologias como Microsoft BitLocker, Linux LUKS ou MacOS FileVault.

Nos casos de locomoção para outros locais, o mesmo deve ser feito de forma discreta, em mochila apropriada e sempre transportada no porta-malas dos veículos.

Ao se ausentar da sua estação de trabalho faça o bloqueio de seu computador, por exemplo: Ctrl + Alt + Del ou + L;

- Equipamentos da Orizon devem ser utilizados exclusivamente para assuntos profissionais relacionados à Orizon;
- Equipamentos não pertencentes à Orizon devem ser conectados somente a rede Guest;
- É vedada a conexão de quaisquer dispositivos pessoais a equipamentos Orizon;
- Exceções somente serão permitidas mediante solicitação para Workplace, e aprovada por Segurança da Informação, após justificativa do gestor.

11.5. Monitoramento

A Orizon se reserva ao direito de monitorar e interceptar o tráfego de redes comum e criptografado oriundos de quaisquer conexões pertencentes à empresa com a finalidade de identificar e bloquear atos potencialmente maliciosos ou suspeitos.

12. SERVIÇOS E CERTIFICAÇÕES

Os terceiros que utilizarem serviços em nuvem, processarem e/ou armazenarem dados da Orizon em seu ambiente devem aderir às diretrizes de Segurança da Informação Orizon. Qualquer necessidade de utilização de serviços de processamento ou armazenamento externo, deve ser comunicada a Segurança da Informação para avaliação de conformidade e aplicação de controles.

É vedada a subcontratação de serviços para suportar processamento e/ou armazenamento de dados da Orizon. Exceções devem ser comunicadas ao gestor e a Segurança da Informação e podem ser somente executadas com aprovação registrada.

13. CONTINUIDADE DE NEGOCIOS E GESTÃO DE BACKUPS

É dever da empresa terceira implementar um programa de continuidade de negócios, para garantir que possíveis incidentes não afetem aos serviços prestados a Orizon, contemplando o plano de recuperação de desastres, com testes nos controles regularmente.

Estabelecer procedimentos de backup regularmente nos dispositivos que armazenam informações da Orizon, com o intuito de prevenir ou reduzir a perda de dados em caso de incidentes, notificando e concedendo acesso à Orizon, mediante solicitação, sobre as medidas de segurança adotadas na transmissão, armazenamento e descarte de dados e informações, incluindo procedimentos seguros de exclusão em mídia e papel.

14. DA LEI GERAL DA PROTEÇÃO DE DADOS

Aplica-se, independentemente de suas atribuições e responsabilidades, a todos os colaboradores da Companhia a Lei Federal nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (“LGPD”), no que se refere ao tratamento de dados realizado pela ORIZON, bem como por terceiros que o fazem em seu nome.

Para os fins de aviso, aplicar-se-ão aos mesmos termos as definições dispostas no artigo 5º da LGPD. Caso você tenha alguma dúvida sobre os termos utilizados neste normativo, sugerimos consultar a tabela:

Termo	Definição
Dado pessoal	Qualquer informação relacionada a pessoa natural, direta ou indiretamente, identificada ou identificável
Dado pessoal sensível	Categoria especial de dados pessoais referentes a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, referentes à saúde ou à vida sexual, dados genéticos ou biométricos relativos a pessoa natural
Titular	Pessoa natural a quem se referem os dados pessoais, tais como antigos, presentes ou potenciais clientes, colaboradores, contratados, parceiros comerciais e terceiros
Tratamento	Toda operação realizada com dados pessoais, como as que se referem: a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão,

	distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração
Anonimização	Processo por meio do qual o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, considerados os meios técnicos razoáveis e disponíveis no momento do tratamento

Os Colaboradores se obrigam a respeitar todos os Normativos da **ORIZON** sempre que utilizarem dados pessoais acessados em razão da relação de trabalho, se abstendo de extrair, copiar, compartilhar, transmitir ou publicar qualquer dado relativo a pessoas naturais, inclusive dados pessoais relacionados a outros empregados, fornecedores, clientes etc.

Esta cláusula de privacidade se aplica em conjunto com as demais políticas aplicáveis à relação entre as partes. Eventuais alterações poderão ser feitas a qualquer momento e serão devidamente comunicadas aos Colaboradores, a fim de garantir máxima transparência.

15. RESPEITO À DIVERSIDADE, EQUIDADE E INCLUSÃO

A Orizon tem o propósito claro de defender a saúde de milhões de pessoas, entregando valor aos nossos clientes por meio da transformação ágil de processos com o uso de inteligência de dados.

Entendemos a nossa cultura como um diferencial competitivo, por isso, a Orizon tem o compromisso de inserir a Diversidade, Equidade e Inclusão (DE&I) como um hábito diário de aprendizado, colaboração e respeito de forma acolhedora e segura para todas as nossas pessoas.

Respeitamos e valorizamos a Diversidade, a Equidade e a Inclusão em todas as nossas atividades e ambientes, como forma de fortalecer a cultura inclusiva, impactar positivamente o clima organizacional, a entrega de valor aos nossos clientes, o bem-estar, a tomada de decisão, a inovação, a produtividade e o relacionamento entre nossas pessoas.

Nossos normativos refletem as atividades diárias e conceitos primordiais da Orizon, como a defesa da saúde com governança, transparência e gestão dos fluxos de trabalho, para que sejamos a cada dia uma melhor empresa para se trabalhar.

O respeito à DE&I, inclusive, está previsto em nossa Cartilha de Diversidade, disponível **na intranet**.

5. RESPONSABILIDADES

RESPONSÁVEL	ATIVIDADE	PRAZO

Área gestora do contrato	Acionar a Segurança da Informação para avaliação do fornecedor sobre serviço ou produto a ser contratado	Sob demanda
	Responder questionário com as informações fidedignas do fornecedor	Sob demanda
	Envio da notificação elaborado pelo jurídico ao fornecedor se houver algum descumprimento da Política de Segurança da Informação ou Contrato	Sob demanda
Jurídico	Elaboração do documento (notificação) ao fornecedor se houver algum descumprimento da Política de Segurança da Informação ou Contrato	Sob demanda aberta via Projuris pela área responsável
Controles internos	Realizar testes periodicamente	Anualmente
Segurança da Informação	Avaliação de Segurança da Informação do fornecedor	Sob demanda

6. CONTROLES DE EMISSÃO, REVISÃO, APROVAÇÃO E HISTÓRICO

◗ Controle de Emissão

NOME	ÁREA	APROVAÇÃO
Caio Felipe Carvalho de Sousa	Segurança da Informação	

◗ Controle de Revisão

NOME	ÁREA	APROVAÇÃO
Marcos de Souza Maurino	Segurança da Informação	
Elger Vinicius Santana Rodrigues	Segurança da Informação	
Dayane Nascimento de Toledo	Governança de TI	

Renato Forte	Controles Internos	
Barbara Silveira Rocha	Compliance	
Rafael Sordi	Privacidade e Proteção de Dados	

Controle de Aprovação

NOME	ÁREA	APROVAÇÃO
Edmundo Maron	Tecnologia da Informação	
Priscila Monteiro Cirino Nóbrega	Segurança da Informação	
Damarys Rodriguez Viganó Montes	Jurídico, Governança Corporativa e P&PD	

HISTÓRICO DAS REVISÕES

VERSÃO	DATA DA EMISSÃO	MOTIVO DAS ALTERAÇÕES	SOLICITADA POR	NOME DO RESPONSÁVEL
01	12/04/2023	Melhoria do fluxo de terceiros.	Tecnologia da Informação	Daniel Barros Sinder
02	04/04/2024	Atualização de Documento.	Segurança da Informação	Daniel Barros Sinder
03	25/02/2025	Atualização de Documento.	Segurança da Informação	Caio Sousa