* OBJETIVO DA POLÍTICA

Estabelecer as diretrizes e orientações necessárias para proteção dos ativos de informação da Orizon em suas diversas formas, de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes, visando preservar o valor e a integridade da organização bem como salvaguardar a confidencialidade, integridade e disponibilidade das informações da companhia.

* 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
1 e 11	Abrangência e Item 1.18: Terceiros e Prestadores de Serviço

* O QUE MUDOU?

PÁGINA	COPIAR AS CLÁUSULAS PRINCIPAIS JÁ ALTERADAS
1 e 11	Abrangência e **Item 1.18**: Terceiros e Prestadores de Serviço

ÍNDICE

1. DISPOSIÇÕES GERAIS

A informação é um dos ativos fundamentais aos negócios da Orizon e a companhia tem a responsabilidade de mantê-los protegidos contra quaisquer ameaças que possam colocar em risco a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

As informações devem ser protegidas de acordo com sua sensibilidade, valor e criticidade. Todas as medidas viáveis de segurança da informação devem ser aplicadas independentemente dos meios em que a informação seja armazenada, processada ou transmitida. Toda informação colocada à disposição dos colaboradores deve ser utilizada apenas para as finalidades de trabalho para a Orizon.

Os colaboradores devem cumprir as diretrizes desta política, realizando periodicamente avaliações de riscos das informações que manuseiam e devem atuar prontamente para reduzir a exposição de seus ativos na ocorrência de incidentes de segurança, também devem monitorar a violação da política de segurança da informação bem como a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações para nossos clientes, colaboradores e demais partes relacionadas. Os colaboradores devem ser conscientizados e ter disponível material de referência e canais que possibilite identificar qual a proteção apropriada para os ativos da informação sob sua responsabilidade.

Os treinamentos e documentações sobre a segurança da informação são de responsabilidade da área de Segurança da Informação e seu conteúdo deve expressar que a segurança da informação é parte importante dos objetivos de negócios da Orizon.

1.1. Diretrizes

Todas as informações geradas e desenvolvidas são consideradas ativos de informação da Orizon.

Os ativos de informação podem estar presentes em diversas formas, tais como: arquivos em diretórios de rede, equipamentos, mídias externas, documentos impressos, sistemas, dispositivos móveis, banco de dados e diálogos.

Independentemente da forma apresentada, compartilhada e/ou armazenada, a informação deve ser utilizada apenas para a sua finalidade, tendo sido devidamente autorizada e estando sujeita a monitoração e auditoria.

Todo o ativo de informação de propriedade da Orizon deve ter um responsável, ser devidamente classificado e adequadamente protegido de qualquer risco e/ou ameaças que possam comprometer o negócio.

Todos os colaboradores, bem como seus processos e tecnologias, devem cumprir as diretrizes de segurança da informação dispostas nesta política, visando a proteção dos ativos de informação.

1.2. Propriedade Intelectual

A propriedade intelectual é composta por bens imateriais de propriedade da Orizon, dentre as quais se incluem informações, patentes, direitos autorais, segredos comerciais, marcas registradas, especificações, desenhos, modelos, cronogramas, exemplos, ferramentas, programas de computador, base de dados, todas as informações produzidas, invenções, códigos de software ou melhorias decorrentes das atividades associadas ao trabalho durante o contrato do colaborador ou mesmo após seu término, por prazo indeterminado e outros direitos de propriedade intelectual da Orizon.

Os inventos, desenvolvimento ou aperfeiçoamento de softwares, sistemas ou outras melhorias feitas pelo colaborador, no exercício de suas atribuições, mesmo que fora do horário de trabalho e fora das dependências da Orizon, desde que relacionados com as atividades da empresa, devem ser comunicados à respectiva liderança.

Todo colaborador é responsável pela preservação da propriedade intelectual da organização, bem como pela observância e respeito à propriedade intelectual de terceiros, nos termos da legislação vigente, cabendo à responsabilização em casos de omissão, dolo ou culpa.

Todas as informações e propriedade intelectual pertencentes à Orizon, ou por ela disponibilizada, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

Devem ser adotadas, pelas respectivas lideranças, todas as medidas cabíveis e legais para proteger a propriedade intelectual, por meio de controles internos e de registro nos órgãos competentes.

1.3. Recursos Corporativos

Todas as informações contidas ou criadas em dispositivos da Orizon ou autorizados para uso dos colaboradores são de propriedade da Orizon e constituem bens da empresa. Dispositivos estes podem ser, mas não se limitando a computadores, notebooks, celulares, tablets ou recursos na "nuvem" abrangendo Internet e Intranet, e-mails, repositórios de arquivos entre outros.

Não é permitido instalar e/ou executar produtos e/ou softwares considerados "piratas" ou gratuitos ("freeware e/ou shareware") em dispositivos Orizon (ex. computadores, notebooks, smartphones e etc.) sem a devida homologação e autorização. A aquisição, instalação e execução de novos programas devem ser homologadas pela área de Tecnologia da Informação e aprovada pela área de Segurança da Informação. O produto deve estar acompanhado de licença legalmente adquirida ou em conformidade com a licença GNU General Public License (GPL), cedida ou autorizada para uso corporativo seguindo suas políticas de uso e privacidade. Caso seja efetuado o uso sem a devida avaliação, a Orizon poderá estar exposta a riscos de pirataria de software e sujeita às sanções e punições legais associadas ao uso indevido.

Os recursos corporativos devem ser utilizados com responsabilidade e para uso de suas atribuições na Orizon, não sendo permitidos os acessos impróprios na Internet, incluindo mas não se limitando a jogos de azar, mensagens de corrente, troca ou armazenamento de conteúdo obsceno, pornográfico, violento, discriminatório, racista, político, religioso, difamatório ou que desrespeite qualquer indivíduo ou entidades), de acordo com as Leis como o Estatuto da Criança (Lei nº 8.069) e o Marco Civil da Internet (Lei nº 12.965).

Os colaboradores devem ter zelo pelos recursos corporativos como computadores, impressoras, celulares e demais equipamentos que ele tenha acesso, podendo sofrer sanções administrativas conforme previsto no código de conduta.

A manutenção e configuração dos recursos físicos (computadores, notebooks, impressoras, celulares) e recursos eletrônicos (softwares) da Orizon são responsabilidade da área de Service Desk em TI, sendo vetado aos demais colaboradores alterarem sua configuração, abrir o equipamento ou alterar componentes.

A Orizon se reserva o direito de monitorar ou de inspecionar o uso dos recursos da empresa e/ou conectado à rede corporativa, que se utilize de informações corporativas – por exemplo, computadores, e-mails, acesso à Internet, conteúdos da marca na Internet, telefones corporativos e informações proprietárias – de acordo com a lei aplicável e procedimentos internos definidos pela área de Segurança da Informação.

Ao ausentar-se de sua estação de trabalho, sala de reunião, ou outros ambientes mesmo que por breve período, o colaborador deve protegê-la contra acessos indevidos com senha de bloqueio. Material impresso deve ser protegido e guardado em local seguro. Material impresso não utilizado deve ser destruído após o seu uso. Cuidados semelhantes se aplicam ao material impresso deixado nos escaninhos de impressoras.

É vedado utilizar qualquer tipo de conexão remota (telefônica, cabo, rede wireless, etc.) nos equipamentos que estejam ao mesmo tempo conectados nas redes locais da empresa.

Um equipamento conectado na rede corporativa da Orizon, não pode se conectar a outra rede simultaneamente. Esta prática pode expor as informações da Orizon e/ou contaminar o ambiente corporativo com vírus.

Todos os incidentes corporativos que envolvam ameaças digitais, incluindo, mas não se limitando a vulnerabilidades, vírus de computador e ataques digitais diretos ou indiretos, devem ser reportados para o CSIRT Orizon de acordo com a Política de Resposta a Incidentes de Segurança da Informação e seus canais de contato vigentes.

1.4. Redes Sociais

Seja consciente com as informações publicadas. O colaborador que infringir alguma diretriz infra mencionada poderá sofrer punições ou sanções descritas no código de conduta.

- Não fale em nome da Orizon, exceto se você possuir aprovação formal da área de Comunicação Corporativa bem como da sua respectiva diretoria;
- Nunca publique informações internas ou confidenciais da Orizon;
- Nunca comente sobre assuntos internos ou confidenciais relacionados à sua função na Orizon;
- Não critique ou faça comentários negativos da concorrência, clientes e parceiros da Orizon;
- Toda e qualquer opinião expressa em mídias sociais é de sua inteira responsabilidade;
- É vetado o acesso às redes sociais por meio da rede corporativa da Orizon, salvo exceções relacionadas ao ambiente corporativo e profissional.

1.5. Continuidade do Negócio

A gestão dos planos de continuidade deve garantir que os serviços essenciais da empresa sejam devidamente identificados, priorizados e documentados para manter a empresa operacional, sem grandes impactos aos clientes, mesmo após um desastre, até o retorno à situação normal, sempre alinhado às necessidades do negócio.

Para tanto, a Orizon dispõe de uma área responsável pela Gestão de Continuidade de Negócio e as diretrizes desse processo estão descritas na Política de Gestão da Continuidade dos Negócios e seus respectivos planos e normativas.

1.6. Gestão de Acesso e Senhas

A gestão de usuários é compartilhada entre Segurança da Informação e Service Desk. Sendo sistemas integrados ao controlador de domínio e ou diretamente ao gerenciador de identidade de responsabilidade de Segurança da informação e demais sistemas e legados ou sem devida compatibilidade, de responsabilidade do Service Desk.

Esta pode ser melhor compreendida na Norma de Controle de Acesso aos Sistemas de Informação.

1.7. Usuários

As credenciais de acesso de colaboradores deverão ser revogadas imediatamente ao término do contrato de trabalho ou prestação de serviços, sendo de responsabilidade dos gestores e/ou da área de Desenvolvimento Organizacional, providenciar estas solicitações para Segurança da Informação.

Os usuários e senhas de rede e sistemas são pessoais e intransferíveis. O colaborador deverá zelar pelas suas credenciais e acessos, trocando a senha, no máximo, a cada 90 dias ou quando suspeitar que a mesma possa ter sido comprometida.

- É de responsabilidade do usuário qualquer ação executada através de sua conta de acesso.

Os usuários e perfis de acessos à rede corporativa e aos sistemas Orizon e terceirizados deverão ser revisados semestralmente pelos gestores ou pontualmente por iniciativa da área de Segurança da Informação.

1.8. Acessos

As solicitações de acessos devem ser formalizadas e serão atendidas após validação dos gestores, que devem verificar se os acessos são compatíveis com as funções e responsabilidades do colaborador.

O colaborador e demais usuários autorizados devem ter acesso somente às informações e recursos que se façam necessários para a realização de suas atividades na Orizon, devendo ser respeitada a segregação de funções.

Todos os acessos concedidos que não sejam necessários para o colaborador desempenhar suas atividades na Orizon devem ser comunicados para TI e Segurança da Informação e removidos imediatamente.

Acessos privilegiados (permissão de acesso além do necessário para execução das atividades do dia-a-dia) e/ou administrativos devem ter sua concessão autorizada pela área de Segurança da Informação em conjunto com a Diretoria responsável pelo colaborador solicitante.

Constitui-se grave violação da Política de Segurança da Informação ter acesso às informações não autorizadas, tentar ou conseguir acesso a qualquer serviço ou informação sem a devida autorização, tentar ou burlar as restrições de segurança, tentar ou prejudicar serviços da Orizon, tentar ou interceptar comunicação de forma não autorizada ou utilizar os recursos da Orizon para atividades não condizentes as suas atribuições profissionais.

1.9. Senhas

A senha é pessoal e intransferível, devendo obedecer aos padrões da Orizon.

É responsabilidade do usuário qualquer ação executada com o seu usuário e senha, constituindo-se grave violação da Política de Segurança da Informação, o compartilhamento dos mesmos.

- O usuário não deve armazenar senha em arquivos digitais, e-mails, papéis ou outras mídias. É recomendado memorizar sua senha.

- Não se deve utilizar senhas consideradas “fracas” como as baseadas em nomes próprios ou dados pessoais tais como nomes, datas, RG, CPF, etc.

- A senha deve ser composta conforme diretrizes estabelecidas na Política de Segurança da Informação Interna.

1.10. Acesso Remoto

É vedado o acesso remoto a recursos conectados na rede corporativa Orizon. Casos de exceção devem ser encaminhados pelo gestor da área à Tecnologia da Informação e aprovado pela área de Segurança da Informação.

1.11. Classificação da Informação

É um processo importante que visa proteger a informação estabelecendo uma classificação mediante a relevância da informação, relacionada ao manuseio, criação, 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.

1.12. Integridade das Informações

As informações da Orizon devem ser corretas, completas, mantidas e descartadas de acordo com os prazos legais e internos.

1.13. Manipulação da Informação

Todas as informações da Orizon devem ser armazenadas na rede corporativa.

É 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 e ambientes de armazenamento em nuvem (Dropbox, OneDrive, iCloud, Google Drive etc.).

1.14. Mesa Limpa

O programa de mesa limpa visa evitar a exposição desnecessária de informações da empresa.

- Não deixe documentos impressos sobre a mesa, nem lembretes (principalmente com senhas) nos monitores e teclados.
- Os documentos impressos e dispositivos externos devem ser guardados em local seguro.
- Sempre apague informações dos quadros antes de deixar a sala de reunião. Se houver informações em papel, faça o descarte utilizando as picotadoras de papel.

1.15. Mesa de Crise

Deve haver um processo de gestão de crises para tratar as crises da empresa, no que se refere à Segurança da Informação, sendo que se caracteriza uma crise quando no mínimo duas áreas sejam afetadas, com impacto na disponibilidade dos serviços, financeiro ou imagem da empresa.

1.16. Uso de Internet e Correio Eletrônico

É vedado o acesso de conteúdo de entretenimento que porventura não seja relacionado às atividades do colaborador.

É vedado utilizar o correio eletrônico corporativo (e-mail) para fins pessoais como, por exemplo: Cadastro em sites de compras, mídias sociais etc.

Os acessos são monitorados e poderão ser bloqueados sem aviso prévio.

1.17. Aviso Legal e Assinatura do Correio Eletrônico

Deve ser utilizado um aviso legal (*disclaimer*) de e-mail automático ao enviar mensagens, aprovados pela Diretoria Jurídica e Segurança da Informação.

- Todos os colaboradores devem configurar sua assinatura no e-mail corporativo conforme o padrão mais atual da empresa.

- Todas as mensagens de e-mail devem ser classificadas como Confidencial, Interna ou Pública, seguindo as regras de Classificação da Informação.

1.18. Terceiros e Prestadores de Serviço

Quando da contratação de terceiros ou prestadores de serviços que tenham colaboradores que venham acessar a rede e dados da Orizon, a área contratante deverá garantir que todos estejam cientes dessa Política. Nesse sentido, o terceiro ou prestador de Serviços, sempre que possível, deverá assinar o Termo de Adesão e Responsabilidade das Políticas Internas Prioritárias da Orizon.

1.19. Segurança Física

1.19.1. Escritórios

Vedado fotografar ou filmar as instalações da Orizon, exceto o espaço reservado para conveniência, salvo por exceções previamente autorizadas.

Todo e qualquer acesso deve ser 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 situação de emergência ou devidamente autorizada pela brigada de incêndio.

1.19.2. Câmeras de Segurança

Os ambientes da Orizon são monitorados por câmeras de segurança, e as gravações são armazenadas conforme as diretrizes da Política de Segurança da Informação Interna.

1.19.3. Uso de 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.

1.19.4. Estações de Trabalho

Os notebooks devem ser protegidos com cadeado físico de segurança, sempre que o colaborador se ausentar. 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 liberação realizada pelo Service Desk, e aprovada por Segurança da Informação, após justificativa do gestor desde que exista controle de mitigação.

1.20. Conscientização

Os colaboradores devem ter conhecimento desta Política e participar de todas as iniciativas de conscientização em relação às boas práticas de Segurança da Informação.

1.21. Aderência a esta política

Colaboradores e áreas devem ser adequar a esta política tempestivamente a partir da data de publicação e/ou revisão.

Com relação à Política de Segurança da Informação Interna, é altamente recomendável que colaboradores novos leiam o documento que contém as diretrizes detalhadas citadas neste documento Público.

2. 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 abaixo:

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.