OBJETIVO

Esta política constitui uma declaração formal da Ozônio acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua custódia, devendo ser observada por todos os seus colaboradores, estagiários, aprendizes e prestadores de serviços. Também é enviada para fornecedores críticos, quando possível, uma vez que o envio não é viável para as plataformas de serviços utilizadas.

Definir as diretrizes de segurança da informação da Ozônio relacionadas à implantação, manutenção, operação e melhoria contínua do Sistema de Gestão da Segurança da Informação (SGSI) e visa:

1. Contribuir com o sucesso no cumprimento de seus objetivos de negócio pela devida proteção da confidencialidade, integridade e disponibilidade da informação, conforme requisitos da norma ISO 27001:2022.
2. Definir as diretrizes para a preservação das informações da Ozônio quanto à confidencialidade, integridade e disponibilidade, e estabelecer instruções normativas de segurança da informação que permitam aos colaboradores e demais partes interessadas, seguir padrões de comportamento desejáveis e aceitáveis de acordo com a legalidade e boas práticas de mercado a fim de mitigar riscos tecnológicos, comportamentais, ambientais e de informação.
3. Direcionar a definição de procedimentos específicos de Segurança da Informação, bem como a implementação de controles e processos para atendimento dos requisitos da mesma;
4. Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de consumidores e parceiros ou de qualquer outro impacto negativo no negócio da Ozônio resultante de uma falha de segurança.

REFERÊNCIAS

Norma **ABNT NBR/ISO/IEC 27001:2022**, Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação —Requisitos

Norma **ABNT NBR/ISO/IEC 27002:2022**, Segurança da informação, segurança cibernética e proteção da privacidade – Controles de segurança da informação.

DOCUMENTOS INTERNOS RELACIONADOS

Manual do Sistema de Gestão da Segurança da Informação

APLICAÇÃO

As diretrizes aqui estabelecidas deverão ser seguidas por todos os seus colaboradores, estagiários, aprendizes e prestadores de serviços da Ozônio, e se aplicam à informação em qualquer formato, digital ou físico.

OBJETIVOS DO SGSI – SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

1. Garantir que todos os colaboradores sob o escopo do SGSI tenham participado do Workshop de Segurança da Informação
2. Atingir um nível de risco aceitável de acordo com nossa Política de Segurança da Informação e seguindo a Metodologia de Gestão de Riscos e Oportunidades
3. Garantir que incidentes de segurança da informação são devidamente registrados, tratados e comunicados alta direção, se aplicável
4. Garantir o cumprimento das legislações aplicáveis
5. Implementação do Sistema de Gestão da Segurança da Informação de acordo com a ISO 27001:2022.

PAPÉIS E RESPONSABILIDADES

1. **Alta Direção**

A constituição da Alta Direção está definida no Manual da Segurança da Informação, que está comprometida com o sistema de gestão de segurança da informação, devendo:

- Estabelecer as responsabilidades e atribuições do Comitê de Segurança da Informação (CSI);

- Assegurar que a política e os objetivos de segurança da informação sejam estabelecidos, de forma compatível com a orientação estratégica da organização;
- Promover a integração dos requisitos do Sistema de Gestão de Segurança da Informação aos processos da organização alcançando a certificação;
- Prover os recursos necessários para o Sistema de Gestão de Segurança da Informação;
- Comunicar a importância da gestão eficaz da segurança da informação, e do cumprimento dos requisitos do Sistema de Gestão de Segurança da Informação;
- Certificar que o Sistema de Gestão de Segurança da Informação alcança seus resultados pretendidos;
- Coordenar e incentivar as pessoas a contribuir com a eficácia do Sistema de Gestão de Segurança da Informação;
- Atender aos requisitos legais, regulatórios e contratuais relacionados ao negócio;
- Promover a melhoria contínua deste SGSI;
- Analisar criticamente o Sistema de Gestão de Segurança da Informação para assegurar sua contínua adequação e efetividade.

2. Comitê de SGSI

Membros: estão definidos no Manual do SGSI

Responsabilidades:

- Consolidar e coordenar a implantação, execução, monitoramento e melhoria do Sistema de Gestão da Segurança da Informação;
- Coordenar as reuniões de análise crítica do Sistema de Gestão da Segurança da Informação, bem como acompanhar os planos de ação resultantes deste fórum;
- Facilitar a conscientização, a divulgação e o treinamento quanto à política e aos procedimentos de segurança da informação;

- Desenvolver um programa de treinamento para os funcionários e prestadores de serviços de forma a conscientizar sobre as responsabilidades de cada um em relação à segurança da informação;
- Gerenciar mudanças organizacionais a fim de garantir os aspectos de disponibilidade, integridade e confidencialidade da informação;
- Informar todos os funcionários e prestadores de serviços sobre a importância da Segurança da Informação, e a necessidade de seguir a política, procedimentos e instruções referentes ao Sistema de Gestão de Segurança da Informação (SGSI);
- Relatar sobre o desempenho do sistema de gestão da segurança da informação para a Alta Direção;
- Sugerir mecanismos para proteção da segurança física e ambiental a fim de prevenir danos e acessos não autorizados à informação;
- Identificar, analisar, avaliar e tratar os riscos de segurança da informação;
- Apoiar na definição de políticas e procedimentos referentes à obrigatoriedade de registro/relato dos eventos e incidentes de segurança por todos os funcionários, bem como as respectivas penalidades pelo não cumprimento deste objetivo;
- Elaborar, atualizar e implantar procedimentos operacionais e os controles de segurança da informação, baseados na instrução normativa;
- Atender e tratar os incidentes de Segurança da Informação registrados
- Conhecer os riscos, legislações e regulamentos, partes interessadas e necessidades dos segmentos de negócio da Ozônio, quanto aos requisitos de segurança da informação;
- Executar projetos e iniciativas visando aprimorar a segurança da informação na Ozônio;
- Requisitar informações das demais áreas da Ozônio, através das gerências, com o intuito de verificar o cumprimento das políticas e procedimentos de segurança da informação e/ou necessidades de capacidade atual e/ou futura;
- Receber, documentar e analisar casos de violação da política e procedimentos de segurança da informação;

- Propor projetos e iniciativas relacionadas à melhoria da segurança da informação;
- Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação;
- Gerir a continuidade dos negócios garantindo a confidencialidade, integridade e disponibilidade da informação, demandando junto às diversas áreas da empresa, planos de continuidade dos negócios, validando-os periodicamente;
- Realizar, sistematicamente, a gestão de riscos relacionados à segurança da informação;
- Adotar mecanismos automatizados, sempre que possível, para gerenciamento, prevenção e detecção de eventos de segurança;
- Adotar processos de autenticação e controle de acesso seguro para os sistemas de informações;
- Deliberar sobre o uso de ferramentas de proteção contra softwares maliciosos, vírus, spam e outros dispositivos que possam ameaçar os sistemas de informação da organização;
- Definir, implantar e testar o Plano de Continuidade de Negócios a fim de garantir a disponibilidade dos sistemas de informações.

Gestores

- Dominar todas as regras de negócio necessárias à criação, manutenção e atualização de medidas de segurança relacionadas ao ativo de informação sob sua responsabilidade (equipe ou unidade de negócio). Os mesmos podem delegar sua autoridade sobre o ativo de informação, porém, continua sendo dele a responsabilidade final pela sua proteção;
- Promover entre os colaboradores a cultura da segurança da informação;
- Cumprir e fazer cumprir as políticas e procedimentos de segurança da Informação;
- Classificar a informação sob sua responsabilidade, inclusive aquela gerada por clientes, fornecedores ou outras entidades externas;

- Utilizar a Gestão de Riscos como instrumento gerencial estratégico para assegurar os requisitos de negócio da organização;
- Enviar ao CGSI, quando solicitado, relatórios sobre as informações e ativos de informação sob sua responsabilidade;
- Manter um controle efetivo do acesso à informação, estabelecendo, documentando e fiscalizando a política de acesso à mesma para os sistemas não gerenciados pelo departamento de Tecnologia da Informação. Tal política deve definir quais usuários ou grupos de usuários têm real necessidade de acesso à informação, identificando os perfis de acesso.
- Selecionar de maneira coerente os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
- Reavaliar, quando solicitado pelo TI, as autorizações dos usuários que acessam as informações sob sua responsabilidade, solicitando o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;
- Fornecer as informações solicitadas pelo Comitê de Gestão de Segurança da Informação e apoiar nas investigações dos incidentes de segurança relacionados às informações sob sua responsabilidade;
- Assegurar que suas equipes possuam acesso e entendimento da política e dos procedimentos de Segurança da Informação;
- Redigir e detalhar, técnica e operacionalmente, os procedimentos de segurança da informação relacionados às suas áreas, quando solicitado pelo CSI.

Colaboradores, estagiários, aprendizes e prestadores de serviços

- Conhecer e cumprir as políticas e procedimentos definidos pela Ozônio, que tratam da Segurança da Informação;
- Zelar continuamente pela proteção das informações da Ozônio ou de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada preservando a confidencialidade, integridade e disponibilidade das informações;

- Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da Ozônio;
- Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Registrar eventuais incidentes de segurança da informação em casos de descumprimento da Política de Segurança da Informação e/ou dos procedimentos de Segurança da Informação conforme política de gestão de incidentes de segurança da informação;
- Manter total sigilo sobre informações obtidas em decorrência da relação empregatícia, sejam elas comerciais ou dados pessoais, sendo vedada qualquer forma de transmissão e uso destas informações em relação à divulgação a terceiros ou para uso pessoal.

DIRETRIZES

As diretrizes de segurança da informação, indicadas abaixo, devem ser respeitadas e obedecidas por todos os colaboradores, estagiários, aprendizes e prestadores de serviços e demais partes interessadas da Ozônio.

Prevenção de ataques

- Gestão de vulnerabilidades: as estações de trabalho e servidores devem ser monitoradas através de ferramentas específicas;
- Registro e monitoramento de logs: o monitoramento é feito e analisado mensalmente;
- Negação de internet: considera-se a internet meio essencial para busca de informações e produtividade do trabalho, portanto, o uso da mesma está liberado sob monitoramento. Os acessos a sites passam por filtro de conteúdo considerado impróprio para o ambiente corporativo e devem ser bloqueados;
- Redes e segregação de redes: grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.

- Conexão à rede de terceiros: a conexão à rede de terceiros deverá ser analisada previamente quanto a sua segurança e necessidade. E quando necessário deverá seguir todos os critérios de segurança, assim como testes de vulnerabilidade, a fim de mitigar riscos quanto à segurança da informação e continuidade do negócio;
- AntiSpam: e-mails deverão ser trafegados por canais seguros;
- Antivírus: estações de trabalho e servidores deverão possuir antivírus instalados e atualizados, e não podem ser desabilitados por usuários comuns;

Gestão de acesso

- Todos os tipos de sistemas que necessitam de acesso lógico deverão possuir um controle formal desde a liberação de acesso até a revogação;
- As identificações e senhas são de uso pessoal e intransferível. Os acessos aos servidores possuem sessões monitoradas e senhas com acessos privilegiados rotacionadas a cada acesso;

Mídias removíveis: mídias removíveis não são permitidas e as exceções são tratadas conforme necessidade.

Descarte e reutilização de equipamentos e mídias: assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou gravados com segurança;

Transferência de informações: A troca de informações com clientes, fornecedores e demais partes interessadas, quando aplicável, deve ser realizada por canais seguros que utilizam criptografia durante a comunicação, se possível.

Gestão da capacidade: Recursos são monitorados quanto a sua capacidade em atender o crescimento da empresa e as operações atuais.

Gestão de incidentes de segurança: Incidentes devem ser gerenciados, catalogados e analisados.

Inventário de ativos e itens de configuração

- Todos os softwares e recursos da empresa devem ser inventariados e controlados pela área de TI, administrativo e/ou desenvolvimento;
- Não é permitida a instalação de nenhum software ou equipamento sem o consentimento da TI, com exceção do depto. Desenvolvimento;
- Não é permitido contratar e utilizar nenhum software para uso organizacional, em nuvem, sem o consentimento da TI ou da Direção;
- A TI deverá ter processos para detecção de softwares instalados;
- Ativos em posse de colaboradores e fornecedores devem ser controlados. Em caso de desligamento ou encerramento de contrato, o ativo deverá ser devolvido conforme procedimento estabelecido pela TI;
- Os softwares devem possuir gestão de suas licenças e uso controlado pela TI e/ou Desenvolvimento. Não é permitida a instalação e execução de software não licenciado ou não homologado pela TI.

Ambiente físico

O acesso nas áreas seguras deve ser protegido e controlado para assegurar que ocorra apenas acesso físico autorizado às informações da organização e outros ativos.

Mesa limpa e tela limpa

As diretrizes de “mesa e tela limpa” devem ser aplicadas em todas as áreas e serem seguidas por todos os colaboradores e prestadores de serviços, tais como:

- Papéis/documentos não fiquem expostos a acessos não autorizados;
- Quaisquer documentos físicos, sejam eles confidenciais, internos ou de uso pessoal, devem ser guardados em locais protegidos, com fechaduras ou outras formas seguras de mobiliário, especialmente fora do horário normal de trabalho;
- Informações classificadas, quando impressas, devem ser imediatamente retiradas da impressora;

- Os colaboradores devem travar/bloquear suas sessões nos computadores toda vez que se afastarem de sua estação de trabalho;
- Equipamentos devem ser protegidos por mecanismo de travamento de tela por senhas, chaves ou outros mecanismos de autenticação quando não estiverem em uso;

Classificação da informação

As informações devem ser classificadas de acordo com as necessidades de segurança da informação da organização com base na confidencialidade, integridade, disponibilidade e requisitos relevantes para as partes interessadas. A sensibilidade dos dados acessados em nosso dia a dia e a maneira de tratá-los conforme a sua classificação, em termos do seu valor, requisitos legais e criticidade, contribui para evitar modificações ou divulgações não autorizadas.

Gestão de backup

O backup das aplicações e servidores devem possuir cópias armazenadas em local diferente do ambiente de produção. Devem ser realizados testes de restore conforme determinado no Manual do TI.

Privacidade e proteção de dados pessoais

A política de privacidade estabelece as diretrizes para a Ozônio a fim de tratar de dados pessoais com privacidade e proteção, assim como determinar as regras sobre a obtenção, uso e armazenamento de tais dados coletados dos usuários, dentro do escopo dos serviços prestados, de acordo com a legislação em vigor.

Fornecedores

Fornecedores, que podem comprometer a confidencialidade, integridade e disponibilidade da informação, devem possuir cláusulas de segurança e sigilo de informação em seus contratos. Os fornecedores devem ser avaliados quanto ao nível de segurança, conforme as diretrizes estabelecidas nesta política, quanto à gestão de acesso, análise de vulnerabilidades e continuidade de negócios.

Continuidade da segurança da informação

A Ozônio possui um plano de recuperação de desastres, o qual é implementado e testado anualmente para gerir a continuidade do negócio da segurança da informação do negócio.

AUDITORIAS

A realização de uma auditoria deverá ser obrigatoriamente aprovada pela Alta Direção e, durante a sua execução, deverão ser resguardados os direitos dos titulares de dados pessoais e observados os deveres quanto à privacidade de dados pessoais.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações de políticas, das normas ou dos procedimentos de segurança da informação, a área de TI poderá realizar monitoramento e controle proativos, mantendo a confidencialidade do processo e das informações obtidas.

Em ambos os casos, as informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

VIOLAÇÕES e MEDIDAS DISCIPLINARES

No caso de violação à política e aos procedimentos de segurança da informação ou a não aderência a esta política poderá ser aplicada penalidade prevista em lei. O não cumprimento dos requisitos previstos nesta política acarretará violação às regras internas da organização e sujeitará o colaborador ao processo disciplinar cabível, conforme determinação do RH.

REVISÕES

Esta política é revisada anualmente ou caso ocorram mudanças significativas, incluindo a avaliação de oportunidades de melhoria e adequação através de análises críticas da Alta Direção garantindo assim a sua contínua pertinência, adequação e eficácia.

CONFLITOS DE INTERESSE

Quaisquer situações decorrentes das informações contidas nesta política ou em outra derivada desta, que possam gerar conflitos internos ou externos à Ozônio deverão ser imediatamente notificadas à Encarregada Oficial de Dados.

QUADRO DE REVISÃO DE CONTEÚDO DO DOCUMENTO

Documento:	Política de Segurança da informação		
Revisão: 1			
Emitente:	JURÍDICO		
Classificação:	INTERNO		
Aprovação:	JULIA SERRUYA		
Revisões:	**Data**	**Histórico**	**Responsável**
v.1	25/11/2024	elaboração	julia serruya