ÓTIMO GESTOR TECNOLOGIA

PSI – Política de Segurança da Informação

PSI – Política de Segurança da Informação

Objetivos

Entendendo o momento que passamos de transformação digital, e o avanço nas legislações de privacidade de dados no Brasil, fomos motivados a estruturar nosso programa de governança de privacidade de dados.

Parte deste programa está baseado na construção de determinação e gerenciamento dos nossos riscos no campo da privacidade de dados. Dentro dos riscos encontramos vulnerabilidades relacionadas ao engajamento das pessoas, tecnologia, processos e nossos parceiros.

Este documento já é a resposta a este trabalho de gestão de riscos, onde queremos mitigar os prejuízos pela ausência de uma política de segurança da informação, que passaremos a chamar de PSI.

Nossa PSI é a declaração do desejo da empresa, as diretrizes para nosso comportamento humano, com relação a segurança da informação.

Nesta PSI estarão previstos os meios adequados e corretos de relacionarmos com a informação de forma segura e preservando os pilares da segurança da informação:

- **Integridade**: garantia que a informação seja mantida em seu estado original, protegendo de alterações indevidas, sejam elas intencionais ou acidentais;
- **Confidencialidade**: garantia de que as informações sejam acessadas apenas pelos usuários autorizados;
- **Disponibilidade**: garantia de que o usuário autorizado encontre a informação disponível sempre que necessário.

Aplicação da PSI

As diretrizes e definições de nossa PSI aplicam-se a todas as pessoas enquadradas abaixo:

- Todos os(as) colaboradores(as) da empresa, independente da função, hierarquia e regime de contratação;
- Todos os prestadores que ofertarem serviços em nome da empresa, estando nas dependências dela;
- Todas as pessoas, independentes de sua relação de negócio com a empresa, estando dentro de nossa estrutura física ou fazendo uso de nossos recursos tecnológicos.

Nossa meta é que todos que estejam dentro de nossa cadeia de serviços, ou dentro de nossa estrutura física e tecnológica, independentemente de seu modelo de contratação, hierarquia ou qualquer outra distinção. Deverão ter em mente em seguir e respeitar nossa política e quando o não realizarem tenham ciência de possível penalização pelas faltas.

Princípios da PSI

Toda informação relacionada a uma pessoa física, coletada e processada no ambiente de trabalho, nas atividades diárias das operações da empresa, são de propriedade exclusiva do titular de dados, nunca da empresa, do colaborador ou do contratado.

Toda informação relacionada a estrutura física, estrutura tecnológica, de produto, de preço ou de quaisquer outras informações da empresa são de propriedade exclusiva da empresa, nunca do colaborador ou do contratado.

A empresa através dos seus investimentos em processos e tecnologia, tem como objetivo preservar a segurança desta informação, para que ela se mantenha íntegra, confidencial e disponível.

Requisitos da PSI

Para que o resultado seja o melhor possível, onde as pessoas se engajem e se comprometam com a política de segurança, é extremamente importante que:

- Todas as pessoas envolvidas nos processos da empresa, recebam treinamento sobre ela, não tenham dúvidas e possuam condições de executá-la;
- Haja um comitê designado para aprovação de alterações futuras desta PSI;
- Todo incidente de segurança que ocorra de forma individual ou coletiva, precisa ser comunicado imediatamente à gerência;
- Assumir que, aquele que tiver conhecimento desta PSI e não a cumprir, estará passível de penalidades, processos administrativos e legais cabíveis.

Responsabilidades nomeadas

Dos gestores tomadores de decisões pela empresa

Ter postura exemplar em relação à segurança da informação, sendo sempre referência no cumprimento desta PSI.

Buscar o engajamento de toda empresa neste objetivo de acelerar e amadurecer a segurança da informação da empresa.

Direcionar orçamento adequado para investir em ações que mitiguem riscos na segurança da informação.

Líderes de pessoas

Ter postura exemplar em relação à segurança da informação, sendo sempre referência no cumprimento desta PSI.

Buscar o engajamento de sua equipe nesta PSI, sempre vigilante e atento a possíveis desvios de comportamento.

Antes de conceder acesso às informações que venham a ser solicitadas, garantir que o dono do acesso tenha ciência dos riscos, da responsabilidade e da missão da empresa em manter a segurança total da informação.

Do comitê de segurança da informação

Deve ser constituído pela liderança da empresa, composto por um gerente de operações, um representante proprietário da empresa, o responsável pela equipe de segurança da informação e responsável pela empresa de governança da privacidade de dados.

Deverá rever esta PSI anualmente, propondo os ajustes e melhorias necessárias.

Este comitê poderá adotar especialistas internos ou externos, para apoiarem nos assuntos que exijam conhecimento específico que o comitê desconheça.

Cabe ao CSI:

- Solicitar pedido de investimentos para segurança da informação.
- Propor alterações nas versões da PSI.
- Avaliar incidentes de segurança e propor ações corretivas.
- Definir as medidas cabíveis nos casos de descumprimento desta PSI.

Dos colaboradores em geral

Entende-se por colaborador neste documento, toda pessoa física, independente da sua forma de contratação, que tenha acesso a informações, sistemas, arquivos, papeis, redes de computadores, equipamentos, ou qualquer outra fonte de dados que for de responsabilidade desta empresa manter a segurança.

É responsabilidade e dever de cada colaborador participar dos treinamentos e ações realizadas pela empresa, para engajá-lo na missão de manter a segurança da informação.

Cumprir tudo o que lhe for atribuído com relação a uso de ferramentas, processos e comportamento na busca da segurança da informação.

Será de inteira responsabilidade do colaborador, deixar de adotar e cumprir esta PSI em sua integra, assumindo para si responsabilidade e autoria de dados que vierem a ser causados, seja para empresa ou terceiros.

Uso de tecnologia

E-mail / Correio Eletrônico

A empresa vai estruturar caixas de e-mail corporativo, e a partir da entrega deste e-mail ao colaborador, o uso e comportamento destes devem seguir assim:

- O uso da caixa de e-mail / correio eletrônico é de uso corporativo exclusivo, para fins de relacionamento e atividades do interesse da empresa.
- É proibido o uso da caixa de e-mail / correio eletrônico para fins particulares.

- É responsabilidade do colaborador manter sua senha eletrônica em sigilo, não podendo compartilhar com outra pessoa, nem mesmo facilitar o descobrimento da senha *(exemplo: anotando em papel exposto em lugar público)*.

Internet / Wi-fi

Nossa empresa entende que o acesso à informação pública através de pesquisa na internet, pode acelerar o desempenho individual e da equipe do colaborador, portanto temos em nossa empresa acesso liberado para rede de wi-fi para dispositivos móveis; portanto o colaborador é responsável pelo acesso, conteúdo e finalidade da pesquisa, assumindo ele a responsabilidade por qualquer dado interno ou a terceiro causado por seu acesso.

Internet / Rede cabeada de computadores

Nossa rede de computadores é privada, não é aberta a visitantes, fica expressamente proibido e passivo de ação administrativa os seguintes itens:

- Mostrar os itens contidos dentro da rede através de uma estação de trabalho para terceiros.
- Compartilhar as telas de sistemas ou diretórios contidos através do uso da rede de computadores.

Estação de Trabalho e Dispositivos móveis da empresa

Toda estação de trabalho e dispositivos móveis cedidos pela empesa para o emprego do colaborador, deve seguir as diretrizes abaixo:

- Não compartilhar senhas e acesso com outros colaboradores e terceiros.
- Não compartilhar o uso do equipamento com outros colaboradores e terceiros.
- Não fazer destes equipamentos, uso pessoal e que venha a comprometer a segurança da informação.

Conexões remotas

Toda conexão remota aos equipamentos, redes e sistemas internos na empresa, deve, obrigatoriamente, ser feita através da VPN (*Virtual Private Network*) disponibilizada pela empresa.

Nuca compartilhar usuário e senha da VPN com outro colaborador ou terceiro, estando passível de processo administrativo-legais e assumindo para si danos à empresa ou a terceiros.

Documentos físicos

Os documentos de papéis sempre ficarão armazenados em local fechado com chave, e o controle da chave será restrito ao grupo de líderes.

Fica proibido o colaborador usar documentos sob responsabilidade da empresa para qualquer outra finalidade que fuja ao processo padrão da empresa, assumindo para si a responsabilidade legal de quaisquer danos.

Quando descartado qualquer papel, de qualquer tamanho, nunca será jogado na lixeira diretamente, antes passará por um picador de papel, para garantir que caso haja dados pessoais neste papel, ele seja eliminado.

Agora que você chegou ao fim da leitura, espero q ue você compreenda a importância da segurança da informação para nossa empresa e clientes, precisamos do seu apoio ao cumprir tudo que foi descrito e também em nos ajudar a deixá-la mais rica e indutiva, encaminhe ao seu líder toda sugestão e contribuição.

Versão e histórico deste documento.

Versão do Documento	***V 1.0.0***
Data do documento	***13/07/2021***
Autores	***Sentinela.Digital e Ótimo Gestor Tecnologia***
Validado e aprovado	***Sergio Bueno***