Política de Segurança da Informação

Documento de Normas Administrativas

Normas Empresa S.A.

Observações

Este documento deve ser atualizado regulamente em períodos, no mínimo, anuais ou quando necessário.

Este documento e suas cópias somente podem ser manipulados e divulgados pelo setor responsável por sua criação e manutenção.

Todos os funcionários da instituição devem ter pleno conhecimento das normas presentes neste documento.

Esta política de Política de Segurança da Informação da Empresa SA deve ser seguida por todos os colaboradores e terceiros. O não cumprimento das diretrizes estabelecidas nesta política pode resultar em medidas disciplinares, conforme previsto nos termos de contrato.

Princípio

Tendo em vista a catalogação dos ativos, sistemas e hardwares internos e externos; juntamente com o mapeamento do fluxo de dados em meio físicos e digitais da Empresa S.A. Estando em anexo no final deste documento, seguimos com normas de segurança da informação afim de garantir a proteção dos dados dos clientes e da empresa.

Resposta a Incidentes

Identificação

Qualquer colaborador da Empresa S.A. ou Terceirizado, caso suspeite de um incidente de segurança, deve reportar imediatamente ao Setor de Segurança da Informação (*SSI*) que irá identificar e confirmar a procedência da informação.

Caso o colaborador ou terceiro tenha ciência plena de que suas suspeitas sejam de fato um incidente de segurança, a não declaração ao setor responsável é passível de *advertência*, prevista nos termos de contrato do colaborador com a diretoria.

Avaliação

Identificado e confirmado o risco como *real* o SSI analisará o impacto e gravidade da situação, tendo liberdade na tomada das medidas de contenção necessárias para e mitigação dos danos presentes ocasionados pelo incidente, até a elaboração da medida de solução.

O SSI deve, obrigatoriamente, documentar o máximo de informações possíveis nessa primeira etapa de ação: mapeando as ameaças, seus fluxos e as soluções de contenção efetuadas.

Passado o primeiro momento o SSI possui um prazo de *72h* para a investigação detalhada e coleta de dados sobre o incidente, priorizando a busca por medidas de solução para a criação de um projeto de resposta ao incidente presente.

O não cumprimento do prazo estabelecido, é passível de punição prevista no contrato com os colaboradores do Setor de Segurança da Informação e a Diretoria.

Comunicação

Com um projeto de solução ao incidente, pensado dentro do prazo, o SSI obrigatoriamente deve comunicar a Diretoria sobre a situação e consultá-la para a aplicação do projeto. A Diretoria deve analisar a proposta de projeto, não sendo necessário concordar com a aplicação total, mas obrigatoriamente sendo necessário aprovar no mínimo o escopo responsável pela neutralização das ameaças.

Caso seja visto como necessário o SSI deve comunicar em nome da Empresa S.A. os colaboradores, terceiros e clientes, sobre que: “Estamos cientes do incidente e medidas já estão sendo tomadas para a sua segurança.”

A Diretoria possui total controle sobre a comunicação do SSI com os demais.

Pós-Incidente

Tendo o incidente sessado, o SSI deve inevitavelmente realizar uma análise das decisões e medidas tomadas durante o ocorrido, documentando e revisando políticas, fluxos e processos da Empresa S.A.

Com a análise em mãos, o SSI será responsável pelo agendamento de no mínimo uma reunião com a diretoria, colaboradores e terceiros, para a treinamento de novas medidas e informe da situação.

O não cumprimento desse processo pós incidente é passível de advertência perante o contrato estabelecido com o SSI e a Diretoria.

Gestão de Identidade e Acesso

ID de Setor

O Setor de Recursos Humanos em conjunto com o Setor de Segurança da Informação são responsáveis pela criação e gestão de *mails* personalizados para cada colaborador e terceiro da Empresa S.A. Cada mail serve como uma identificação do colaborador e seu setor, seguindo o padrão: *<nomedocolaborador>.<setordocolaborador>@empresasa.co*

O RH possui obrigação de comunicar ao SSI sempre que um colaborador ou terceiro, entrar, sair ou mudar de setor dentro da instituição. Para que o SSI realize as ações necessárias no controle de acesso.

O uso destes mails de identificação por parte dos colaboradores ou terceiros para fora dos dispositivos da instituição é passível de punição severa perante o contrato estabelecido entre as

partes com a Empresa S.A. O RH tem total liberdade para tomar tais punições caso o SSI confirme a infração.

Fica sobre responsabilidade direta do RH e do SSI determinar (em conjunto) quais documentos, programas e sistemas cada mail terá permissão de visualizar, editar e administrar.

Controle de acesso

A Autenticação Multifatorial (*MFA*) necessita ser aplicada em todos os *mails* dos colaboradores e terceiros da Empresa S.A. O SSI deve dispor de ferramentas de criação e gestão de senhas FORTES, em conforme com a LGPD e as condutas da ISO27001.

As senhas devem ser armazenadas em uma ferramenta de *gerenciador de senhas* certificada, possuindo uma cópia de segurança armazenada em uma ferramenta de *cofre de senhas* certificada, essa só podendo ser acessada pela Diretoria.

Apenas o SSI e Diretoria devem possuir acesso as senhas dos mails, sendo passível de d*emissão por justa causa* qualquer colaborador ou terceiro que divulgar ou ter acesso irrestrito a tais senhas. Tendo o RH total autonomia para aplicar tal ação caso o SSI confirme a infração.

O acesso e configuração de mails institucionais em novos dispositivos, somente podem ser feitos em máquinas da Empresa S.A. que possuem registro prévio de suas Identificações de sistema e produto. Sendo de total autonomia do Setor de Segurança da Informação, a remoção, bloqueio ou formatação de dispositivos fora do escopo de IDs registrado.

Auditoria

O SSI possui total autonomia na utilização de ferramentas de monitoramento regular dos sistemas e canais de comunicação em conforme com a LGPD. Onde estes possuem restrição de acesso apenas para a Diretoria e SSI. Os colaboradores devem ter plena ciência e aceitar, mediante contrato, o monitoramento constante para fiz de segurança.

Treinamento

O Recursos Humanos em conjunto com o SSI carece de organizar mensalmente, no mínimo, um encontro para treinamento e atualização dos colaboradores e terceiros sobre as novas condutas e políticas internas da Empresa S.A. da LGPD e das normas da ISO27001.

Gestão de Risco

Considerando a gestão ID de Setor em conformidade com as normas da metodologia RBAC, seguimos com a referida gestão:

Identificação de Ativos Críticos

A Empresa SA deverá manter um registro atualizado de todos os ativos críticos, incluindo dados dos clientes, sistemas de manutenção e informações financeiras. Esse registro deve possuir acesso restrito apenas a Diretoria, RH e SSI.

O vazamento dos dados de registro, a colaboradores ou externos não autorizados é passível de punição perante o contrato estabelecido com o SSI e a Diretoria.

Avaliação de Riscos

Serão realizadas avaliações regulares de riscos, seguindo a metodologia da ISO 27001, para identificar ameaças, vulnerabilidades e a probabilidade de ocorrência. A avaliação levará em consideração as funções específicas dos colaboradores pré-estabelecidas pelo parágrafo “ID de Setor” presente na clausula “Gestão de Identidade e Acesso”.

A regularidade do referido deve manter no mínimo períodos de 15 dias entre os relatórios de Avaliação de Risco.

Mitigação de Riscos

Com base nas avaliações de risco, serão implementadas medidas de mitigação, incluindo controles técnicos, organizacionais e treinamento, alinhados com as melhores práticas discutidas e acordadas entre o SSI e setor de Tecnologia da Informação. Sendo obrigatória a constante busca pela otimização da segurança dos Ativos Críticos.

Controle de Acesso

A gestão de identidade e acesso, conforme descrito na política correspondente, será integrada ao processo de gestão de risco para garantir um controle efetivo sobre o acesso aos ativos críticos. Utilizando-se como normas complementares a política, o método RBAC e normas em conformidade com a ISO27001.

Auditoria e Monitoramento

Será conduzida uma auditoria regular dos controles de segurança implementados, utilizando ferramentas aprovadas pelo SSI, conforme autorizado pela LGPD. A auditoria será realizada com restrição de acesso apenas para a Diretoria e SSI.

Os setores de RH e TI devem colaborar com o SSI para a realização das auditorias que possuem obrigatoriamente uma regularidade semanal.

O não cumprimento da regularidade estabelecida, é passível de punição prevista no contrato com os colaboradores do Setor de Segurança da Informação e a Diretoria.

Resposta a Incidentes

A gestão de risco incluirá a preparação para incidentes de segurança, conforme estabelecido na política de resposta a incidentes. O SSI terá autonomia para tomar medidas de contenção imediatas em caso de incidentes, seguindo as diretrizes previamente estabelecidas.

Comunicação

Em casos de incidentes de segurança, a comunicação com a Diretoria será obrigatória. A Diretoria terá controle sobre a comunicação externa, conforme descrito na política de resposta a incidentes.

O SSI nunca deverá realizar uma comunicação interna sem antes a aprovação da Diretoria. O não cumprimento dessa norma, é passível de suspensão do colaborador determinada pela Diretoria e RH.

Pós-Incidente

Após a resolução de um incidente, o SSI será responsável por conduzir uma análise pós-incidente, documentando as lições aprendidas e revisando as políticas, fluxos e processos da Empresa SA. Visando a otimização da segurança dos Ativos Críticos.

O não cumprimento desse processo pós incidente é passível de advertência perante o contrato estabelecido com o SSI e a Diretoria.

Melhoria Contínua

A gestão de risco será sujeita a revisões periódicas, com o objetivo de identificar oportunidades de melhoria e atualizar os controles de segurança conforme necessário, buscando a otimização regular da segurança dos Ativos Críticos.

Conformidade com Regulamentações

Todas as atividades de gestão de risco estarão em conformidade com as regulamentações aplicáveis, incluindo a LGPD. A Empresa SA compromete-se a proteger os dados dos clientes de maneira ética e legal.

Ass.: Leonardo Rodrigues 08/12/23