Política de Cyber Segurança

HISTÓRICO DE REVISÕES

Número da edição	**Elaborador** (Nome/data)	**Revisor** (Nome/data)	**Descrição da alteração**
01	Edemar H K Luccezen 16/04/2018	Nandor Feher 18/01/2018	Criação da política de Cyber Segurança

TERMOS E ABREVIAÇÕES

Cyber Segurança: Conjunto de medidas tecnológicas que protege computadores, programas, redes e dados de qualquer invasão indevida.

Ativos de informação: Conhecimento ou dados que tem valor para uma organização.

Engenharia Social: Termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão.

SIEM: (Security Information and Event Management) Conjunto de ferramentas computacionais, processos e procedimentos com a finalidade de coletar, armazenar, processar, monitorar e correlacionar logs de outros sistemas de informação.

OBJETIVO

Esta Política de **Cyber Segurança** descreve todos os fatores que devem estar em vigor para proteger os **ativos de informação,** por meio do tratamento, preventivo ou não, de qualquer ameaça que põem em risco a informação que é processada, armazenada ou transportada.

PÚBLICO-ALVO

Esta política destina-se a todos os colaboradores da Positivo Tecnologia, sejam eles: funcionários, estagiários, prestadores de serviços (terceiros), parceiros de negócio, visitantes da empresa ou qualquer pessoa que tenha acesso a qualquer ativo de informação.

RESPONSABILIDADES

Segurança da Informação

Realizar o levantamento e a classificação dos ativos da empresa.
Avaliar o grau de risco e de vulnerabilidade desses ativos, testar suas falhas e definir o que pode ser feito para aperfeiçoar a segurança.
Avaliar possíveis brechas de segurança e recomendar as correções necessárias.
Criar, e solicitar a cada área, um plano de ação para recuperação de desastre e continuidade de negócio.
Revisar as políticas de segurança para readequação dos cenários periodicamente;

Administração de Servidores

Aplicar as correções recomendadas pela área de Segurança da Informação.
Manter os servidores e seus sistemas e serviços atualizados e inventariados.

Frontend e Telecom

Manter todas as estações e dispositivos móveis atualizados, e inventariados.
Aplicar as correções recomendadas pela área de Segurança da Informação.
Informar possíveis falhas ou vulnerabilidades encontradas;

Colaboradores

Utilizar os recursos fornecidos seguindo todas as premissas encontradas nas políticas de Segurança da Informação e de Cyber Segurança;

1 DIRETRIZES

1.1 Princípios de Cyber Segurança

Para assegurar a proteção do ambiente tecnológico, é necessário adotar medidas preventivas:

- Manter todos os softwares atualizados;
- Informar e conscientizar todos os colaboradores sobre os perigos cibernéticos;
- Proteger e prevenir a infraestrutura contra os ataques virtuais.
- Prevenir e detectar vulnerabilidades;
- Proteger as informações alocadas em ambientes virtuais;
- Prevenir acessos de pessoas não autorizadas aos dados corporativos e/ou sigilosos.

1.2 Diretrizes gerais de Cyber Segurança

Para identificar os riscos e tomar as medidas apropriadas, a área de Segurança da Informação da Positivo Tecnologia irá executar, juntamente com os administradores dos processos e sistemas, varreduras regulares em toda a infraestrutura (rede, portas, sistemas, serviços, firewall, switches, servidores internos e externos, computadores pessoais, dispositivos móveis, etc.), bem como realizar testes de **Engenharia Social**.

Serão coletados os dados das tecnologias, realizadas simulações de ataques internos e externos e verificadas as melhores práticas e conceitos para melhoria das não conformidades encontradas.

1.2.1 Auditorias

Serão realizadas auditorias sob demanda, proveniente da plataforma de **SIEM** e de outros softwares utilizados, além de auditorias arbitrárias e aleatórias realizadas pela análise das ferramentas de segurança.

1.2.2 Definições

Para realização do processo de auditoria definimos que:

- Todo o conteúdo armazenado em qualquer dispositivo corporativo pode ser analisado sem autorização;
- Dispositivos pessoais utilizados para o uso corporativo devem estar autorizados mediante aceite do Termo de Utilização de Dispositivos Móveis, e podem ter seus dados analisados sem restrições. Dispositivos pessoais não autorizados serão bloqueados e o colaborador poderá ser notificado;
- Todos os acessos aos sistemas, arquivos ou recursos devem passar por uma aprovação e conter um número de registro de chamado, seguindo as premissas necessárias por seus respectivos administradores, mesmo que a necessidade seja proveniente da realização de testes;
- Todos os softwares utilizados podem ser auditados conforme homologação da área de Segurança da Informação;
- Será auditada a utilização dos links ofertados, analisando utilizações fora de escopo, desvios de processo, ou qualquer caso que porventura tenha seu consumo fora dos padrões aceitáveis;
- Todo compartilhamento de credencias será analisado;
- Qualquer desvio necessário a esta política deverá ser autorizada pelo gestor de Segurança da Informação, e pelo gestor da área de negócio requisitante;
- Qualquer desvio não autorizado seguirá o *item 1.4* **Desvios à Politica Vigente.**

1.2.3 Premissas

Para a realização das auditorias, a área de Segurança da Informação tem como premissas:

- Manter a confidencialidade das informações obtidas, não podendo repassa-las sem a permissão do cliente ou superior;
- Proteger a propriedade intelectual de todos;
- Nunca usar um software obtido de forma ilegal ou antiética;
- Usar as informações do cliente ou empregador de forma consciente e sigilosa;
- Não realizar práticas fraudulentas;
- Ter uma conduta ética e competente todo o tempo;
- Promover a pratica do hacker ético para mitigação de riscos, sem realizar nenhuma atividade maliciosa;
- Não violar nenhuma lei.

1.3 Normas

Para a implantação e aplicação da **Cyber Segurança**, serão adotas as normas **ISO/IEC 27001 e ISO/IEC 27002,** destinadas a gestão e controle da Segurança da Informação.

1.4 Desvios à Politica vigente

O não atendimento às recomendações da área de Segurança da Informação deverá ser justificado mediante termo de aceite do risco apresentado, desde que este não seja risco de nível crítico. Todo desvio estará sujeito a sanções, que podem variar desde uma advertência até o desligamento do colaborador da Positivo Tecnologia, inclusive por justa causa, de acordo com a quantidade de recorrências e/ou criticidade do desvio realizado.

São exemplos de desvios que podem ocasionar sanções:

- Não aplicação intencional de correção já definida.
- Utilização de técnicas não homologadas para burlar bloqueios aplicados.
- Não cumprimento do **SLA** acordado para correções críticas sem justificativa;
- Desvio a qualquer um dos itens apresentados no *item 1.2.2* **Definições.**

1.5 Gestão de Cyber Segurança

Para uma adequada Gestão de Cyber Segurança da Positivo Tecnologia, estabelecemos os seguintes controles:

1.5.1 Gestão de Ativos da Informação

Os ativos da informação serão verificados periodicamente, visando controle e prevenção.

1.5.2 Gestão de Acessos

Serão realizados testes de acessos a sistemas e recursos a fim de prevenir falhas e acessos não autorizados.

1.5.3 Gestão de Senhas

Em caso de suspeita de compartilhamento ou vazamento de senhas, a conta será forçada a realizar a alteração da senha, ou em casos graves poderá ter seu acesso bloqueado de imediato.

1.5.4 Gestão de Riscos

Os riscos serão identificados por meio de análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Positivo Tecnologia, para que sejam recomendadas as proteções adequadas.

1.5.5 Tratamento de Incidentes de Segurança da Informação

Os incidentes deverão ser tratados por um plano recuperação de desastre e continuidade de negócio.

1.5.6 Conscientização em Segurança da Informação

Serão realizados testes de **Engenharia Social** com o intuito de conscientizar, capacitar e fortalecer a cultura da Segurança da Informação.

1.6 Declaração de Responsabilidade

Os Colaboradores e Prestadores de Serviços diretamente envolvidos pela Política de **Cyber Segurança**, devem estar cientes das implicações desta.

2 DOCUMENTOS RELACIONADOS

Esta Política Corporativa de Segurança da Informação é complementada por normas e procedimentos específicos de Segurança da Informação disponíveis no portal http://gsi.positivo.corp/, em conformidade com os aspectos legais e regulamentares, das quais a empresa está sujeita.

3 ÓRGÃO RESPONSÁVEL

A área de Segurança da Informação é responsável por manter e atualizar esta política, bem como por manter a confidencialidade, integridade e disponibilidade das informações, por meio de ações de conscientização e treinamento, processos e também por meio de monitoramento e auditoria das ações realizadas por cada colaborador.