POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUAPE

2020

SUMÁRIO

DEFINIÇÕES E ABREVIAÇÕES

A) POLÍTICA: a intenção e orientação geral formalmente expressa pela administração.

B) INFORMAÇÃO: é o dado que tem significado em algum contexto para quem o recebe.

C) COLABORADOR: todo o funcionário, estagiário, terceirizado, coordenador, diretor, presidente, conselheiro, membro de comitê, secretário e assessor de Suape.

D) TERCEIROS: toda pessoa física ou jurídica que não seja colaboradora de Suape ou que não seja por ela única e integralmente contratada, mas que seja contratada para auxiliar no desempenho de suas atividades, tais como parceiros, consorciadas, representantes, fornecedores, prestadores de serviço em geral, consultores temporários, agentes ou terceiros que atuem em nome de Suape.

E) AMEAÇA: causa potencial de um incidente indesejado, o qual pode resultar no dano a um sistema ou organização.

F) ATIVO: qualquer item que tenha valor para a organização.

G) AUTENTICIDADE: propriedade de uma entidade ser o que afirma que é.

H) CONFIABILIDADE: propriedade de consistência dos comportamentos e resultados desejados.

I) EVENTO DE SEGURANÇA DA INFORMAÇÃO: Ocorrência identificada de um estado de um sistema, serviço ou rede que indique uma possível violação da política de segurança da informação ou falha de proteção, ou uma situação previamente desconhecida que possa ser relevante em termos de segurança.

J) EXPOSIÇÃO: é a circunstância de estar exposto aos prejuízos oriundos de um agente ameaçador.

K) GESTOR DA INFORMAÇÃO: colaborador que exerce a chefia de área na empresa Suape, responsável pela informação em sua área de competência.

L) ENGENHARIA SOCIAL: tentativa de extrair informações de uma vítima, usando informações corretas ou nome de pessoas conhecidas. Ex: fingir ser colaborador de Suape, fornecedor ou funcionário da Coordenadoria de TI.

M) MALWARE: software indesejado.

N) SPAM: mensagem indesejada.

O) VÍRUS: pequeno programa de computador que propositalmente se replica.

P) SPYWARE: programa que coleta informações no computador e as envia para outro.

Q) BACKUP: cópia reserva.

R) PC: políticas Complementares.

S) PSI: Política de Segurança da Informação.

T) EXPLOIT: é o nome dado a qualquer programa que aproveite uma vulnerabilidade que o sistema alvo ofereça.

U) TM: gerenciamento unificado de ameaças, abreviado como UTM *(Unified Threat Management)*, é um termo de segurança de informações que se refere a uma única solução de segurança, e normalmente um único dispositivo, que oferece várias funções de segurança em um único ponto da rede.

V) ATAQUE DDOS: esse tipo de ataque consiste em um computador mestre utilizar vários (até milhões de) outros computadores para atacar determinado site.

W) RANSOMWARE: é um tipo de software malicioso que bloqueia o acesso a um sistema de computador ou dados, geralmente, criptografando-o, até que a vítima pague uma "taxa de resgate" para o atacante. Em muitos casos, o pedido de resgate vem com um prazo e se a vítima não paga a tempo, os dados são perdidos para sempre.

X) ENDPOINT: antivírus adotado por SUAPE.

Y) MOVIMENTO LATERAL: ocorre quando um invasor usa contas não confidenciais para acessar contas confidenciais. Os invasores usam o movimento lateral para identificar os administradores em sua rede e saber quais computadores eles podem acessar. Com essas informações e outras movimentações, o invasor pode tirar proveito dos dados em seus controladores de domínio.

Z) DNS: Domain Name System, ou Sistema de Nomes de Domínios. É um computador com uma espécie de banco de dados que relaciona o endereço "nominal" (site de SUAPE, por exemplo) com o endereço real (número de IP, de Internet Protocol) para poder acessá-lo.

AA IP: Protocolo de Internet (em inglês: I*nternet Protocol, ou o acrónimo IP*) é um protocolo de comunicação usado entre todas as máquinas em rede para encaminhamento dos dados.

BB SSL: É um sistema que permite a troca de informações entre dois computadores, de modo seguro. SSL

CC HTTP: HyperText Transfer Protocol é um protocolo que permite que o computador troque informações com o servidor que abriga o site. Isso quer dizer que quando são conectados sob o protocolo, o computador pode receber e enviar qualquer conteúdo de texto.

O maior problema com o HTTP é que algumas conexões, como é o caso do Wi-Fi, são propícias para que uma pessoa mal-intencionada, como um hacker, acesse o conteúdo e intercepte os dados recebidos, deixando então a conexão HTTP insegura para o usuário.

DD HTTPS: Hyper Text Transfer Protocol Secure, HTTP com camada de proteção para quem está acessando o seu site.

EE VPN: Virtual Private Network (Rede Virtual Privada) é a comunicação entre computadores e outros dispositivos que têm acesso restrito a quem tem as credenciais necessárias. E pode ser usado para acesso de qualquer lugar conectado aos sistemas.

FF LGPD: Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados e Privacidade

PRINCÍPIOS

São princípios para o Sistema de Segurança da Informação a Confidencialidade, a Integridade e a Disponibilidade, conforme a ISO 27.001:2013. Esses princípios devem nortear todas as atividades dentro de Suape, a fim de que as informações sejam protegidas no âmbito desta empresa.

Confidencialidade: propriedade em que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados.

Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.

Integridade: propriedade de proteger a exatidão e a integridade dos ativos.

Além dos princípios basilares, devem ser observados os princípios correlatos da Segurança da Informação, tais como o princípio da autenticidade, o princípio do não repúdio e o princípio da utilidade.

OBJETIVOS

O objetivo da Política de Segurança da Informação de Suape - PSI é, através de um conjunto de princípios, nortear e dar as diretrizes sobre a gestão da segurança da informação em Suape, devendo ser observada pelos colaboradores de Suape e terceiros, conforme indicado no item 5, visando à proteção e segurança das informações.

DIRETRIZES

I - A informação de Suape deve ser protegida de maneira a garantir sua confidencialidade, integridade e disponibilidade;

II – O acesso à informação deverá possibilitar o desempenho das atividades relativas à Suape, atendendo à legislação em vigor;

III – O usuário é responsável pelo acesso realizado;

IV – A informação apenas deve ser acessada em decorrência da necessidade da função desempenhada ou outra situação formalmente permitida;

V – As informações devem ser classificadas em relação ao seu nível de sigilo com o objetivo de descrever o tratamento que deve ser dado à informação, indicando a forma de segurança que é necessária;

VI – Devem ser realizadas ações de treinamento, disseminação e conscientização de qualquer pessoa que possua vínculo com Suape para entender suas responsabilidades e se apropriar da Política de Segurança da Informação da empresa;

VII – Qualquer incidente relativo ao sistema de informação deve ser reportado à Coordenadoria de Tecnologia da Informação, a fim de que ações sejam adotadas;

VIII – Devem-se priorizar medidas preventivas quando comparadas com os controles reativos;

IX – O acesso à informação deve ser concedido com base na necessidade do conhecer;

X - A obtenção de determinadas informações, consideradas sensíveis, apenas será permitida mediante a assinatura de termo de confidencialidade;

XI - Para funções que envolvam confidencialidade, tais como, mas não apenas, controle interno, auditoria interna, será necessária a assinatura de termo de confidencialidade;

XII – Todos os equipamentos disponibilizados devem ser utilizados no exercício das atividades de trabalho;

XIII – O e-mail corporativo pode ser monitorado, bem como pode ser realizado o controle de acesso em relação ao uso da internet no ambiente de trabalho;

XIV – Devem ser observadas e respeitadas as normas estabelecidas no ISPS CODE – O Código Internacional para Segurança de Navios;

XV – Deve-se respeitar e assegurar o sigilo das informações, obtidas em razão do exercício das atribuições do cargo, mesmo após a conclusão do trabalho;

XVI – Deve-se zelar pelo seu local de trabalho, de modo a conservá-lo limpo, sem exposição de informações.

ABRANGÊNCIA

A Política de Segurança da Informação deve ser observada pelos colaboradores, terceiros, menor aprendiz e todos os indivíduos que, direta ou indiretamente, utilizam sistema, infraestrutura e informações de Suape, estejam elas em qualquer meio, eletrônico ou físico.

RESPONSABILIDADES

a) Conselho de Administração

I – Aprovar a Política de Segurança da Informação, após a análise pela Diretoria Colegiada de Suape, bem como acompanhar e monitorar a sua execução.

b) Diretoria Colegiada de Suape

I – aprovar, previamente, a Política de Segurança da Informação, e submeter, posteriormente, à aprovação do Conselho de Administração de Suape.

c) Diretor de Administração e Finanças

I – Dirigir, supervisionar e coordenar as atividades relativas à Segurança da Informação.

d) Coordenadoria de Tecnologia da Informação

I - Garantir a implantação e manutenção do processo de Segurança da Informação;

II – Coordenar a atualização da Política de Segurança da Informação (PSI), propondo revisão e políticas complementares, bem como os procedimentos que assegurem as ações da Política de Segurança da Informação.

e) Grupo de Trabalho sobre LGPD

I – Articular projetos e ações voltados à adequação à Lei Federal nº 13.709/2018 (LGPD) no âmbito de Suape.

f) Gestores das áreas

I – Gerenciar as informações sobre sua competência.

g) Colaborador

I – Os colaboradores de Suape devem zelar e proteger a Segurança da Informação em Suape.

h) Coordenadoria Jurídica

I – Dar todo apoio necessário, do ponto de vista jurídico, para implantação e funcionamento da Política de Segurança em Suape.

i) Coordenadoria de Recursos Humanos

I – Informar o desligamento de colaboradores de Suape à Coordenadoria de Tecnologia da Informação;

II – Manter ações de treinamento e educação dos usuários em Segurança da Informação, podendo contar com apoio do Conselho de Ética, com o Compliance, Auditoria Interna e Tecnologia da Informação;

j) Unidade de Gestão de Riscos e Controle Interno - Compliance

I – Participar e colaborar com os processos de segurança da informação e a adequação de Suape à LGPD;

k) Auditoria Interna

I – Monitorar a adequação de Suape à LGPD e verificar a adesão de Suape aos critérios de Segurança da Informação estipulados na Política de Segurança da Informação e suas políticas complementares;

l) Coordenadoria de Comunicação

I – Manter ações de conscientização e educação dos usuários em Segurança da Informação, podendo contar com apoio do Conselho de Ética, com o Compliance, Auditoria Interna, Recursos Humanos e Tecnologia da Informação.

m) Usuários da Informação

I – Zelar e Proteger a segurança da Informação em Suape;

II - Conhecer e cumprir integralmente a política de segurança da Informação e suas Políticas Complementares;

III - Comunicar à Coordenadoria de Tecnologia da Informação qualquer evento que viole esta política;

IV - Assinar os termos de uso e afins que se fizerem necessários, assumindo responsabilidades;

V - Responder pela inobservância da Política de Segurança da Informação.

ACESSO FÍSICO E LÓGICO

SUAPE compromete-se a possuir um conjunto de equipamentos, softwares e regras de utilização de sistemas informatizados para evitar o acesso indevido e/ou a perda de integridade de seus dados e as intrusões em seus sistemas e ataques cibernéticos que possam interromper total ou parcialmente o funcionamento geral da administração portuária e do complexo industrial.

SUAPE utilizará soluções de appliances multi-ameaças de tecnologia UTM para segurança de redes de computadores, instalados nas localidades do Centro Administrativo, na Torre de Controle e no prédio da Unidade de Segurança, visando segurança e conexão de todos os prédios do Porto Organizado que fazem parte da rede de Tecnologia da Informação do Porto de SUAPE.

O Firewall fornece segurança avançada e alto desempenho para proteção em toda a superfície de ataque digital. Os firewalls corporativos diminuem a complexidade ao fornecer visibilidade total aos usuários, dispositivos, aplicativos e ameaças na rede com a capacidade de aplicar proteção avançada contra ameaças em qualquer lugar da rede.

Os serviços de segurança dos appliances protegem contra ameaças, malwares e sites mal-intencionados usando inteligência de ponta para manter sua rede protegida contra ataques cibernéticos avançados.

a) Conexões de ponto de rede clandestinos: todos os computadores da rede de SUAPE deverão estar conectados à Racks que possuem chave e ficam em salas com acesso controlado. Todo novo dispositivo conectado na rede precisa se autenticar no Firewall/UTM para conseguir se comunicar com a internet. Além disso, todos os dispositivos e servidores físicos e virtuais devem possuir software de antivírus Endpoint instalados e atualizados com defesa de ataque em rede, com bloqueio de ameaças como ataques de força bruta, roubos de senha, exploits de rede e movimentos laterais antes que eles sejam executados.

b) Uso de softwares não autorizados: todos as máquinas em uso na empresa serão gerenciadas por políticas definidas no controlador de domínio e apenas usuários com perfil de administrador poderão instalar softwares e demais aplicativos.

c) Contaminação por vírus: Toda rede de computadores da empresa será gerenciada por equipamentos do tipo UTM. O UTM servirá como o núcleo de seus recursos de segurança. Desta forma, é possível conseguir a proteção e a conformidade principais do firewall. Além dessa proteção de borda, todos os dispositivos e servidores físicos e virtuais possuirão software antivírus *Endpoint* instalados e atualizados, sendo mais uma barreira contra possíveis ataques cibernéticos.

d) Furtos de dispositivos: Os dispositivos portáteis utilizados por colaboradores serão protegidos por senha e ainda haverá a possibilidade de exclusão e bloqueio de arquivos através do software Endpoint.

e) Acessos não autorizados: Todos os sistemas utilizados na empresa possuirão controle por login e senha e registro de log com data e hora de todos os acessos/alterações. Quando for detectado acesso indevido a qualquer tipo de informação restrita ou sigilosa, imediatamente será feito o bloqueio, no tempo em que a chefia do colaborador será informada.

f) Controle de tentativa de ataque DDOS: Os equipamentos utilizados possuirão a tecnologia que protege contra ataques conhecidos e de dia zero com latência muito baixa. Também incluirá ferramentas abrangentes de análise e geração de relatórios.

g) Ransonware e Malware: A empresa adotará duas principais tecnologias para bloquear esse tipo de ameaça. A primeira é no UTM, que detecta ataques desconhecidos usando análise dinâmica e fornece mitigação automatizada para parar ataques direcionados. Protege também contra explorações conhecidas, malware e sites maliciosos usando inteligência de ameaças contínua.

Outra tecnologia de prevenção é através do Endpoint, que possui uma solução de segurança adaptativa em camadas, que fornece múltiplas capacidades *anti-ransomware*, fazendo todas as suas camadas trabalharem juntas para a prevenção, detecção e remediação/limpeza.

BACKUP

Os backups são essenciais para deixar as informações seguras e não perder nenhum dado em caso de ataques. Diversos desastres ou tentativas de ataques cibernéticos podem acontecer e, com o backup, todos os dados estarão disponíveis para serem recuperados na sua integridade, sem muitos estragos.

Todos os backups são feitos de forma automática utilizando softwares de mercado com essa finalidade. Essas rotinas são executadas preferencialmente fora do horário comercial, nos períodos em que não há nenhum ou pouco acesso de usuários ou processos aos sistemas de informática.

Esses backups são executados diariamente e ficam armazenados em Storage, dentro do Datacenter, exclusiva para essa finalidade. Todos os dados de File Server, Máquinas Virtuais e Banco de Dados são mantidos em Backup.

Além do Backup local, existe uma rotina específica para armazenar os mesmos arquivos na nuvem.

Todo acompanhamento diário de logs e testes de restauração é feito por uma empresa terceirizada e seguindo todos os critérios de sigilo descritos em contrato.

SISTEMAS DE APOIO À GESTÃO

São atenuados os riscos de ataques cibernéticos que prejudiquem os serviços, sistemas e processos de uso de e-mails, documentos administrativos, Website do Porto e gestão de projetos devido ao armazenamento e hospedagem deste estarem nos Data Centers gerenciados pela Agência de Tecnologia da Informação do Governo do Estado de Pernambuco (ATI).

O Porto de Suape adota o Sistema Colaborativo com ferramentas de automação de processos e escritórios mantendo arquivos em Sites seguros e contingenciados em Ferramenta na Nuvem.

ACESSO REMOTO

O Firewall/UTM adotado em SUAPE dispõe de recursos para fornecer acesso seguro e confiável a redes corporativas e aplicativos de praticamente qualquer local remoto conectado à internet (VPN). A autenticação de dois fatores também pode ser usada para fornecer camada adicional de segurança. Esse acesso é feito utilizando o aplicativo cliente do UTM instalado nos computadores dos usuários com permissão para fazer tal acesso.

PENALIDADES

As transgressões às normas desta Política de Segurança da Informação, respeitado o devido processo legal, ocorrerão, administrativamente, na medida da Lei nº 6.123/1968, e, penal e civilmente, no âmbito da legislação pátria. O não cumprimento desta Política poderá ensejar punições contratuais também.

POLÍTICAS COMPLEMENTARES

As políticas complementares, que irão detalhar os procedimentos específicos, serão anexadas a esta Política, à medida que forem elaboradas.

CASOS OMISSOS

Casos omissos serão avaliados pela Coordenadoria de Tecnologia de Informação para posterior deliberação da Diretoria Colegiada de Suape;

APROVAÇÃO E REVISÃO

Esta política foi aprovada pela Diretoria Colegiada de Suape, e, posteriormente, pelo Conselho de Administração.

Esta Política será revisada de acordo com a demanda que se fizer necessária.

SUAPE
Complexo Industrial Portuário
Governador Eraldo Gueiros

Secretaria de
Desenvolvimento
Econômico

GOVERNO DO ESTADO
PERNAMBUCO
MAIS TRABALHO, MAIS FUTURO.