IT-ONE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Índice

1. HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
02/06/21	1.0	Criação do documento	Peterson Pires

2. TERMOS UTILIZADOS EM SEGURANÇA DA INFOMAÇÃO

- Ameaça

  Risco potencial de um incidente indesejado que pode resultar em dano para um sistema ou para a IT-One.

- Acesso à informação

  É o ato de um usuário ter contato com a informação, seja por meio físico(papel) ou digital e ter conhecimento dela.

- Acesso seguro ou Acesso controlado

  É o acesso à informação feito com a existência de controles que buscam garantir que:

  - apenas as pessoas que devam ter acesso a uma determinada informação, tenham este acesso;
  - seja registrado tudo que é feito com a informação;
  - sejam considerados os tipos de acesso, como leitura, alteração ou remoção da informação;
  - foram tomados cuidados para garantir a integridade da informação.

- Acesso remoto

  - É a forma de acesso ao ambiente computacional, na qual o usuário não está utilizando diretamente a infraestrutura da rede interna da IT-One. Normalmente esse acesso se faz quando o usuário está fora das instalações da IT-One como por exemplo em casa ou em viagem.

- Ambiente de tecnologia

  - É o ambiente que utiliza a tecnologia para o tratamento da informação. É o mundo virtual. Neste caso as informações estão gravadas nos discos (e outras mídias) e para a utilizarmos precisamos de equipamentos de tecnologia e de programas que são executados neste ambiente.

- Ambiente de desenvolvimento de sistemas

    - É o ambiente computacional destinado ao desenvolvimento, à manutenção e alteração dos sistemas de informação da IT-One. As informações deste ambiente têm por objetivo possibilitar a construção dos programas, a realização de testes e a simulação de situações de erro que possam ser identificadas para garantir uma excelente qualidade funcional dos programas aplicativos utilizados nos serviços prestados.

- Autenticação do usuário

    - É a validação de que a pessoa é realmente a pessoa que diz ser. Esta autenticação pode ser feita pelo uso único ou em conjunto de algo que o usuário sabe (senha), algo que o usuário tem (cartão) ou algo que o usuário é (biometria).

- BYOD (Bring Your Own Device)

    - Traduzido literalmente como “traga seu próprio dispositivo móvel”, refere-se à utilização de dispositivos pessoais no ambiente de trabalho.

- Confidencialidade

    - É um dos objetivos da segurança, que indica que a informação somente estará disponível para o usuário previamente autorizado a acessar a informação em função de necessidade de seu exercício profissional perante a IT-ONE.

- Continuidade do negócio

    - É o objetivo da segurança da informação de que o recurso continuará disponível e operante ao longo do tempo, mesmo que ocorram situações que impactem este recurso.

- Cópia de segurança

    - É a cópia das informações de um determinado ambiente (computacional), que tem por finalidade a possibilidade de recuperação desses dados quando da ocorrência de situações que gerem indisponibilidade das informações originais.

- Criptografia da informação

- É um processo matemático que transforma a informação original em uma sequência de informação que ninguém entende (garante a confidencialidade) e depois permite retornar a informação original (que todos entendem).

- Custodiante de recurso

  - É a pessoa que fica responsável por um determinado recurso e tem a obrigação de cuidar bem deste para que funcione adequadamente ao longo do tempo.

- Dado pessoal

  - Significa qualquer tipo de informação identificável referente a um determinado indivíduo ou através da qual determinados indivíduos possam ser identificados, como nome, RG, CPF e endereço ou um ou mais fatores relacionados à identidade fisiológica, mental, econômica, racial, cultural ou social, ou outras características/atributos pessoais.

- Desastre físico

  - É uma situação que causa indisponibilidade ou alteração indevida de recursos de informação, causada por elementos da natureza ou equipamentos e ambientes construídos pelo homem.

- Desastre lógico

  - É uma situação que causa indisponibilidade ou alteração indevida de recursos de informação causada por ação no ambiente computacional, através de programas ou ações que alteram indevidamente as informações, porém não modificando as características do meio físico onde essas informações estão armazenadas.

- Disponibilidade da informação

  - É um dos objetivos da segurança da informação que busca garantir que a informação esteja acessível para o usuário quando este necessitar utilizar o serviço, respeitando os acordos de nível de disponibilidade previamente acertados.

- Gestor(dono) da Informação

  - É a pessoa que autoriza ou nega o acesso à informação pelo usuário. Essa autorização ou negação é em função da avaliação que o gestor faz sobre a real necessidade de o usuário acessar a informação.

- Gestor do Usuário

- É a pessoa, normalmente um coordenador/gerente, que tem a responsabilidade de indicar que o usuário é uma pessoa verdadeira na organização e realiza determinadas tarefas. É a pessoa que autoriza a inclusão ou a exclusão do usuário dos sistemas da organização. Cada usuário deve ter seu gestor. O Gestor do Usuário garante que existam apenas usuários válidos no ambiente da organização.

- Grupo de acesso à informação

  - É um grupo de pessoas que possuem o mesmo direito de acesso à informação. Em vez de terem um acesso individual, é criado um grupo com o acesso comum que todos necessitam.

- Identificação do usuário

  - É a sequência de caracteres que representará o usuário no ambiente computacional. Exemplo: matrícula, nome, CPF.

- Incidente

  - É qualquer ocorrência que altere a normalidade do serviço. Normalmente associamos incidente a uma ocorrência que acarreta impacto negativo ao serviço.

- Indisponibilidade parcial

  - É a não disponibilidade de um recurso ou de um conjunto de recursos de um ambiente, porém uma maior parte dos recursos continua funcionando. Não existe uma ruptura/quebra total de recursos.

- Indisponibilidade total

  - É a não disponibilidade do serviço motivada pela ruptura de um recurso ou de um conjunto de recursos. Neste caso é necessário a substituição do recurso principal por outro recurso alternativo. Normalmente as atividades e a operacionalização do serviço ou negócio da organização serão feitas em outro ambiente físico.

- Integridade

  - É um dos objetivos da segurança da informação que garante que a informação mantenha a sua representação original e não foi corrompida por aspectos de ambiente físico ou de falhas no ambiente lógico.

- Internet

- É o ambiente virtual onde diferentes computadores de várias partes do mundo se comunicam através de protocolos de entendimento comum, permitindo a troca de informações e o compartilhamento de conhecimento.

- Não-repúdio

  - Ato de evitar que uma entidade negue a execução de uma ação.

- Nível de sigilo/confidencialidade da informação

  - Indica o tratamento mais rígido ou menos rígido que deve ser dado à informação, em relação ao seu uso. Para cada grau de sigilo ou confidencialidade da informação, deve haver um conjunto de regras indicando o tratamento desta informação em várias situações, seja no ambiente computacional ou no ambiente convencional.

- Perfil de acesso à informação

  - Próximo da definição de grupo de acesso. Porém, perfil de acesso está mais relacionado a um perfil da função profissional que o usuário realiza.

    Exemplo:

    GERENTES. Neste caso teremos o perfil gerente previamente definido com vários acessos autorizados. Quando alguém na IT-One for contratado como gerente, ele receberá os acessos do perfil gerente.

- Poder de acesso à informação: leitura, alteração, acesso de retirada do recurso

  - Quando é dado um acesso à informação deve-se indicar o poder desse acesso. Alguns usuários vão apenas ler, mas outros vão poder alterar. E ainda há aqueles que poderão apagar a informação.

- Processo de segurança da informação

  - É o processo que implanta, desenvolve, mantém, atualiza e planeja a segurança da informação na IT-One.

- Recurso de informação

  - São elementos que armazenam, processam, transmitem ou tratam da informação. Variam do mundo tecnológico como discos, fitas e equipamentos, até o ambiente convencional: papel, nossas mentes.

- Recurso físico que suporta a informação

- É o recurso físico que possui a informação. Exemplo: uma folha de papel. O papel é o recurso, mas a informação é aquilo que está desenhado no papel.

- Registro de acesso à informação

  - É o registro de quando a informação foi: acessada, alterada, gravada, removida. É muito importante para o caso de saber o que aconteceu com a informação. E é também a garantia de auditabilidade.

- Regras de proteção da informação

  - São os procedimentos de segurança da informação que o usuário deve ter conhecimento explícito e deve seguir.

- Requisitos de segurança

  - São os controles que devem existir para que o uso da informação aconteça de forma segura. Os requisitos de segurança estão descritos nos regulamentos de segurança da informação e em documentos técnicos relativos à proteção da informação.

- Senha de autenticação

  - É um conjunto de caracteres que deve ser de conhecimento apenas do usuário. Dessa forma, quando o usuário digitar a senha o ambiente computacional validará se está correta. Se estiver correta o ambiente computacional assumirá que a pessoa que está digitando essas informações é o usuário da identificação.

- Servidor (computador)

  - É o computador ou o conjunto de computadores que suportam o ambiente corporativo de uma organização. Normalmente a responsável pelos servidores da organização é a área de TI.

- Situações de contingência

  - São situações que tornam indisponível a informação (ou outro recurso). Podem ser causadas por problemas da natureza (chuva, raios, terremoto) ou ação humana (roubo, atentado, erro).

- Sistemas aplicativos

  - São sistemas desenvolvidos para atender de maneira específica as organizações. Exemplo: folha de pagamento, controle de estoque, etc.

- Usuário

    - É a pessoa que utiliza a informação. É qualquer pessoa que, devidamente autorizada, pode acessar os sistemas de informação, seja para exercer atividade profissional para a IT-One ou para interagir com a IT-One como cliente.

- Usuário Cliente

    - É o usuário que utiliza como cliente os serviços de sistemas de informação disponibilizados pela IT-One.

- VPN (Rede Privada Virtual)

    - Conexão estabelecida sobre uma infraestrutura pública (internet), usando protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas.

3. OBJETIVO

Tornar a segurança da informação como um dos elementos fundamentais no planejamento estratégico IT-One;

Definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente IT-One.

Difundir os aspectos relacionados à Segurança da Informação na IT-One.

As orientações aqui apresentadas são os princípios fundamentais e representam como a IT-One exige que a informação seja utilizada.

4. ABRANGÊNCIA

Esta política se aplica:

- a todos os usuários (conselheiros, presidente, diretor, empregado, estagiário ou prestador de serviço) que utilizam as informações da IT-One;

- a todas as organizações que compõem o Grupo IT-One.

5. IMPLANTAÇÃO

O Departamento de Segurança da Informação, juntamente com as áreas de TI e/ou IMS e as chefias das áreas da IT-One desenvolverão ações contínuas e necessárias para a implementação deste regulamento, ficando o Departamento de Segurança da Informação responsável pela coordenação dessas ações.

O Departamento de Segurança da Informação será envolvido quando do desenvolvimento de novos sistemas de informação e validará se os requisitos básicos de segurança serão seguidos.

6. DIRETRIZES E REGRAS

6.1 - O bem 'informação'

A informação utilizada pela IT-One é um bem que tem valor. A informação deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

6.2 - O Gestor(dono) da Informação (GI)

Cada informação deverá ter o seu Gestor que será indicado formalmente pela diretoria responsável pelos sistemas que acessam a informação.

O Gestor da Informação é a pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação.

6.3 - Confidencialidade da informação

O Gestor da Informação classificará o nível de confidencialidade e sigilo da informação baseando-se nos critérios estabelecidos na Norma de Classificação da Informação.

A confidencialidade da informação deve ser mantida durante todo o processo de uso da informação e pode ter níveis diferentes ao longo da vida dessa informação.

6.4 - Utilização da informação e recursos

A liberação de acesso da informação para os usuários será autorizada pelo Gestor da Informação, que considerará a necessidade de acesso do usuário e o sigilo da informação para a realização dos objetivos da IT-One.

O acesso da informação deve ser autorizado apenas para os usuários que necessitam da mesma para o desempenho das suas atividades profissionais para a IT-One.

Cada usuário deve acessar apenas as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso consciente a ambientes não autorizados será considerada uma falta grave.

O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Este acesso acontece através da identificação e da autenticação do usuário. Os dados para a autenticação do usuário devem ser mantidos em segredo e possuem o mais alto nível de classificação da informação.

Os recursos de tecnologia da IT-One disponibilizados para os usuários têm como objetivo a realização de atividades profissionais. A utilização dos recursos da IT-One com finalidade pessoal é permitida, desde que seja em um nível mínimo e que não viole a Política de Segurança da Informação e o Código de Conduta e Ética da IT-One.

6.5 - Proteção da informação

Toda informação da IT-One deve ser protegida para que não seja alterada, acessada e destruída indevidamente. Os locais onde se encontram os recursos de informação devem ter proteção e controle de acesso físico compatível com o seu nível de criticidade.

6.6 - Continuidade do uso da informação

Toda informação utilizada para o funcionamento da IT-One deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção equivalente ao local principal. Esta informação deve ser suficiente para a existência de planos de continuidade de negócio. A criação das cópias de segurança deve considerar os aspectos legais, históricos, de auditoria e de recuperação do ambiente. Os recursos tecnológicos, de infraestrutura e os ambientes físicos onde são realizadas as atividades operacionais do negócio da IT-One devem ser protegidos contra situações de indisponibilidade e devem ter planos de continuidade de negócio. A definição e implementação das medidas de prevenção e recuperação, para situações de desastre e contingência, devem ser efetuadas de forma permanente e devem contemplar recursos de tecnologia, humanos e de infraestrutura. Elas são de responsabilidade da diretoria gestora dos recursos, contando com o apoio e validação da Gerência de Segurança da Informação.

7. POLÍTICAS COMPLEMENTARES

A Política de Segurança da Informação (PSI) no âmbito da IT-One está estruturada com as Políticas Complementares indicadas a seguir, que tratam da gestão dos recursos tecnológicos e devem ser atendidas conforme sua especificidade:

7.1 PC01 – Política de Uso de Senhas

Estabelecer critérios para a criação de senhas fortes, proteção dessas senhas, bem como a frequência de suas atualizações.

7.2 PC02 – Política de dispositivos móveis (BYOD)

Estabelecer critérios que permitam a utilização de dispositivos móveis, incluindo os dispositivos pessoais dos colaboradores que assim desejarem.

7.3 PC03 – Política de uso da internet

Estabelecer as exigências mínimas de segurança da informação para o uso seguro da Internet.

7.4 PC04 – Política de uso do Correio Eletrônico

Estabelecer critérios que determinem as exigências mínimas de segurança para uma comunicação através do correio eletrônico institucional.

7.5 PC05 – Políticas de Resposta a Incidentes de Segurança da Informação

Estabelecer medidas a serem tomadas nos tratamentos de incidentes envolvendo a segurança das informações. Incidentes de segurança da informação em eventos que podem resultar em perda, dano ou acesso não-autorizado às informações.

7.6 PC06 – Política de classificação da informação

Estabelecer padrões na determinação de quais informações podem ser divulgadas fora da IT-One, bem como a sensibilidade relativa de informações que não devem ser divulgadas sem a devida autorização.

7.7 PC07 – Política de acesso remoto

Estabelecer regras e requisitos para acesso externo à rede da IT-One e minimizar o risco potencial para danos que possam resultar do uso não autorizado.

7.8 PC08 – Política de backup corporativo

Estabelecer padrões para a cópia e restauração, com a finalidade da continuidade e disponibilidade das informações, observando a relevância e criticidade destas.

7.9 PC09 – Política de Combate a Softwares Maliciosos e Controle de Vulnerabilidades

Estabelecer critérios claros e objetivos para monitoramento, análise e resposta de incidentes causados por softwares maliciosos como, vírus, worm....

7.10 PC10 – Política de Gestão de Ativos

Estabelecer padrões e critérios que garantam a eficiência e segurança no controle de ativos da IT-One.

7.11 PC11 – Política de Controle de Acesso

Estabelecer critérios que garantam o controle efetivo de acesso aos recursos físicos e virtuais da IT-One, sem prejudicar a continuidade do negócio.

7.12 PC12 – Política de Criptografia

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e integridade da informação.

7.13 PC13 – Política de Retenção e Descarte

Estabelece critérios claros sobre as retenções e descarte dos dados pessoais que são coletados pela IT-One.

7.14 PC14 – Política de Privacidade

A Política de Privacidade destina-se a esclarecer quais informações coletamos, porque as coletamos e como você pode atualizar, gerenciar, exportar e excluir essas informações.

8. DOCUMENTAÇÃO

Todos os procedimentos que possibilitam a proteção da informação e a continuidade do negócio devem ser documentados, de tal forma que possibilite que a IT-One continue a operacionalização desses procedimentos, mesmo na ausência do usuário responsável.

9. CONCLUSÃO

A utilização das informações do ambiente de tecnologia ou do ambiente convencional pelos usuários da IT-One deve estar de acordo com os documentos institucionais “Código de Conduta”, “Política de Privacidade – Dados Pessoais” e “Conduta Ética e Conflito de Interesses”. Todos os usuários devem conhecer e entender esses documentos.

A segurança e proteção da informação é uma responsabilidade contínua de cada usuário da IT-One em relação às informações que acessa e gerencia. Todos os usuários devem utilizar a informação da IT-One, de acordo com as determinações desta Política de Segurança da Informação.

O não cumprimento desta política e/ou dos demais instrumentos normativos que complementarão o processo de segurança constitui em falta grave, e o usuário está sujeito a penalidades administrativas e/ou contratuais. A Gerência de Segurança da Informação é a área responsável pela existência efetiva do processo de proteção e segurança da informação da IT-One.

Informações adicionais poderão ser solicitadas diretamente à Segurança da Informação ou encaminhadas através do Service Desk.