IT-ONE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PC06 - Política de Classificação da Informação

1. HISTÓRICO DE VERSÕES

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

INTRODUÇÃO

A informação é considerada como patrimônio pela IT-One e, em virtude de sua importância, deve ser protegida adequadamente. Para tanto, faz-se necessário que a informação seja classificada segundo sua relevância, através de níveis de sigilo correspondentes ao seu ciclo de vida.

A classificação da informação é o processo que define seu nível de confidencialidade, considerando a sua importância na organização e os impactos decorrentes dos acessos das pessoas, áreas organizacionais e público em geral. Além disso, observa-se também quais processos devem ser seguidos para garantir a proteção das informações.

A informação deve ser classificada da seguinte maneira:

- Pública: quando for de uso livre e seu conteúdo possa ser divulgado publicamente;

- Interna: quando a informação tramitar internamente na esfera da IT-One e não estiver claramente classificada como pública, reservada, secreta ou ultrassecreta e a divulgação de seu conteúdo possa prejudicar a instituição;

- Reservada: quando a informação tramitar no âmbito da IT-One e cujo conteúdo, se divulgado, possa comprometer a IT-One;

- Secreta: quando pode ser acessada apenas por um grupo restrito de pessoas, de forma que sua divulgação não autorizada pode implicar em perdas financeiras ou prejudicar a reputação/imagem da IT-One;

- Ultrassecreta: quando dirigida a um grupo extremamente limitado de pessoas, nominalmente identificadas. A divulgação de seu conteúdo pode permitir acesso a informações estratégicas e pôr em risco os colaboradores ligados a ela, além de causar sérios prejuízos à IT-One.

Cada informação possui seu ciclo de vida correspondente aos seus respectivos momentos vividos e que são evidentes quando os ativos físicos, tecnológicos e humanos fazem uso da informação, garantindo processos que suportam a operação da organização.

Neste sentido, o ciclo de vida da informação merece atenção, pois corresponde às situações em que a informação é exposta a ameaças, colocando em risco sua integridade. Assim, podemos destacar quatro fases relativas ao ciclo de vida:

a) 1ª fase: quando a informação é criada e manipulada, seja ao folhear papéis, digitar informações recebidas ou até mesmo o uso de senha de acesso para autenticação;

b) 2ª fase: quando a informação é armazenada, seja em banco de dados, anotações em papel, mídia óptica etc.;

c) 3ª fase: quando a informação é transportada, seja por correio eletrônico, postal, telefone etc.;

d) d) 4ª fase: quando a informação já não é mais útil e deve ser descartada (ex.: depositada em uma lixeira, apagada do banco de dados, etc.)

e) Considerando o ciclo de vida da informação em relação ao descarte, deve-se observar os prazos máximos de restrição de acesso, conforme descrição a seguir:

I. Informação Ultrassecreta: 15 (quinze) anos;
II. Informação Secreta: 10 (dez) anos;
III. Informação Reservada: 5 (cinco) anos;
IV. Informação Interna: conforme determinar o gestor da área ou superior;
V. Informação Pública: conforme determinar o gestor da área ou superior.

O nível de classificação poderá mudar durante o ciclo de vida, de forma que uma informação “ultrassecreta” poderá ser considerada “secreta” posteriormente, por exemplo, desde que o seu responsável assim estabeleça, respeitando o ciclo de vida da reclassificação.

OBJETIVO

Esta política tem por objetivo garantir que a informação receba um nível adequado de proteção, de acordo com a sua importância para a IT-One. Institucionalizar que o gestor de área tenha a atribuição de gestor da Informação, auxiliando na proteção da informação, através da solicitação do nível de confidencialidade, conforme atribuição e competência, bem como a necessidade de sua proteção e disponibilização, conforme sua classificação. Isso servirá de base para evitar que informações sigilosas sejam disponibilizadas indevidamente.

ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da IT-One, quais sejam: funcionários servidores ou comissionados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da IT-One. Todos esses colaboradores serão tratados nesta política como usuários.

DIRETRIZES DA CLASSIFICAÇÃO DAS INFORMAÇÕES

1. Diretrizes

a) O gestor de cada área tem como competência e dever solicitar a classificação do sigilo das informações.

b) A indicação da classificação da Informação deve levar em consideração:

   i. A necessidade de proteger as informações de acordo com sua importância e suas consequências, caso estas sejam comprometidas;
   ii. As regulamentações e exigências legais;
   iii. As obrigações contratuais.

c) A classificação da informação deve existir, independentemente do formato, local e da mídia de armazenamento;

d) As concessões de acesso aos ambientes computacionais, pastas de rede, dispositivos de rede e outros que possibilitem acessos às informações da IT-ONE, devem ter aprovação dos seus respectivos gestores de área ou superior;

e) O respectivo gestor de área ou superior deve realizar periodicamente um processo de análise de classificação, para avaliar se as informações permanecem com o mesmo nível de sigilo ou se deve ser solicitada a reclassificação;

f) Nos casos em que houver a combinação de várias informações diferentemente classificadas, as informações resultantes devem adotar o nível mais alto de classificação dentre as combinadas;

g) Os direitos de acesso dos usuários às informações devem ser periodicamente revistos e atualizados pelos seus respectivos gestores de área ou superior.

h) É preciso atenção especial para evitar que informações sensíveis não sejam solicitadas, erroneamente, pelo gestor da área, como classificação pública, de forma que devem ser adotados critérios para se decidir quais informações podem ser classificadas como públicas;

i) As informações de caráter reservada, secreta ou ultrassecreta devem ter sua classificação estampada;

j) As Informações que não possuírem classificação de forma explícita, não eximem o gestor da área ou superior da responsabilidade de avaliá-las e solicitar para que sejam classificadas adequadamente;

k) A utilização e o acesso das informações produzidas ou recebidas devem ser feitos de acordo com sua classificação, atribuindo aos respectivos usuários as permissões mínimas necessárias ao desempenho de suas atividades;

l) O processamento, armazenamento, transmissão e eliminação da informação devem ser feitos de acordo com sua classificação;

m) A transmissão da informação classificada como reservada, secreta ou ultrassecreta deve ocorrer apenas com aprovação da autoridade responsável e nos limites por ela estabelecidos, de forma a não identificar seu conteúdo, nem classificação;

n) O armazenamento da informação deve considerar medidas de proteção lógica e física, de acordo com sua classificação, de forma que a informação seja acessada apenas por usuários autorizados;

o) A eliminação da informação deve ocorrer de forma permanente, seguindo procedimentos determinados, e que possam ser utilizados fragmentadores de papel, desmagnetizadores de disco rígido, dentre outros recursos;

p) A informação deve ser classificada antes de ser divulgada, sob o risco de perder o caráter sigiloso, se for o caso;

q) O tratamento das informações pessoais deve ser transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas.