DECRETO NÚMERO 8081 DE 28 DE DEZEMBRO DE 2022

Institui a Política de Segurança Da Informação e Comunicação – POSIC no âmbito da Administração Direta e Indireta na Prefeitura Municipal De Ubatuba e dá outras providências.

FLAVIA CÔMITTE DO NASCIMENTO (FLAVIA PASCOAL), Prefeita Municipal da Estância Balneária de Ubatuba, Estado de São Paulo, no uso das atribuições que lhe são conferidas por Lei; e,

D E C R E T A:

Art. 1º Fica instituída a Política de Segurança da Informação - POSIC no âmbito da Administração Direta e Indireta na Prefeitura Municipal de Ubatuba, elaborada pela Secretaria Municipal de Tecnologia da Informação, cujo texto foi aprovado pelo Comitê de Segurança da Informação e Proteção de Dados – CSegInfo, instituído pela Portaria Nº 977 de 07 de dezembro de 2022.

Art. 2º Para efeito deste Decreto ficam estabelecidas as Diretrizes e Normas constantes no Anexo I.

Art. 3º Este Decreto entra em vigor na data de sua publicação.

PAÇO ANCHIETA – Ubatuba, 28 de dezembro de 2022.

FLAVIA CÔMITTE DO NASCIMENTO
(FLAVIA PASCOAL)
Prefeita Municipal

THIAGO LAMOSA
Secretário Municipal de Tecnologia da Informação

Publicado no Diário Oficial da Municipalidade e no mural do Paço Municipal, registrado e arquivado nos procedimentos pertinentes, junto a Divisão de Acervo da Secretaria Municipal de Administração, nesta data.

SMTI/dcb.

Política de Segurança da Informação e Comunicação POSIC - 2022

PREFEITURA MUNICIPAL DA ESTÂNCIA BALNEÁRIA DE UBATUBA

PREFEITA

Flávia Pascoal

SECRETÁRIO MUNICIPAL DE TECNOLOGIA DA INFORMAÇÃO

Thiago Lamosa

Dezembro 2022

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
19/12/2022	1.0	Política de Segurança de Informação e Comunicação - POSIC

Os trabalhos para elaboração estão registrados no processo administrativo SA/14715/2022, juntamente com o Plano Diretor de Tecnologia da Informação – PDTI.

ELABORAÇÃO

EqPOSIC – Equipe Técnica para Elaboração da Política de Segurança da Informação e Comunicação – POSIC	
Luiz Antonio de Oliveira Serpa	Diretor de Gestão de Tecnologia da Informação
Diego Guimarães Ferreira de Sá	Analista de Tecnologia da Informação
Eduardo Calil Faiçal	Analista de Tecnologia da Informação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - POSIC

Sumário

Glossário

Contas de administrador	Contas dedicadas com privilégios escalados e usadas para gerenciar aspectos de um computador, domínio ou toda a infraestrutura de tecnologia da informação da empresa. Os subtipos comuns de contas de administrador incluem contas root, contas de administrador local e de administrador de domínio e contas de administrador de rede ou dispositivos de segurança.
Aplicação	Um programa, ou grupo de programas, hospedado em ativos corporativos e projetado para usuários finais. As aplicações são consideradas um ativo de software neste documento. Os exemplos incluem aplicações web, de banco de dados, baseadas em nuvem e móveis.
Sistemas de autenticação	Um sistema ou mecanismo usado para identificar um usuário por meio da associação de uma solicitação de entrada a um conjunto de credenciais de identificação. As credenciais fornecidas são comparadas às de um arquivo em um banco de dados de informações do usuário autorizado em um sistema operacional local, serviço de diretório de usuário ou em um servidor de autenticação. Exemplos de sistemas de autenticação podem incluir active directory, autenticação multifator (MFA), biometria e tokens.
Sistemas de autorização	Um sistema ou mecanismo usado para determinar os níveis de acesso ou privilégios de usuário/cliente relacionados aos recursos do sistema, incluindo arquivos, serviços, programas de computador, dados e recursos de aplicações. Um sistema de autorização concede ou nega acesso a um recurso com base na identidade do usuário. Exemplos de sistemas de autorização podem incluir active directory, listas de controle de acesso e listas de controle de acesso baseadas em funções.
Ambiente em nuvem	Um ambiente virtualizado que fornece acesso conveniente à rede sob demanda a um pool compartilhado de recursos configuráveis, como rede, computação, armazenamento, aplicações e serviços. Existem cinco características essenciais para um ambiente de nuvem: autoatendimento sob demanda, amplo acesso à rede, pool de recursos, elasticidade rápida e serviço medido. Alguns serviços oferecidos por meio de ambientes de nuvem incluem Software as a Service (SaaS), Platform as a Service (PaaS) e Infrastructure as a Service (IaaS).
Banco de dados	Coleção organizada de dados, geralmente armazenados e acessados eletronicamente a partir de um sistema de computador. Os bancos de dados podem residir remotamente ou no local. Sistemas de gestão de banco de dados (SGBDs ou DMSs) são usados para administrar bancos de dados e não são considerados parte de um banco de dados para este documento
Dispositivos de usuário final	Ativos de tecnologia da informação (TI) usados entre os membros de uma empresa durante o trabalho, fora do expediente ou qualquer outra finalidade. Os dispositivos de usuário final incluem dispositivos móveis e portáteis, como laptops, smartphones e tablets, bem como desktops e estações de trabalho. Para os fins deste documento, os dispositivos do usuário final são um subconjunto dos ativos corporativos.
Ativos corporativos	Ativos com potencial para armazenar ou processar dados. Para os fins deste documento, os ativos corporativos incluem dispositivos de usuário final, dispositivos de rede, dispositivos não computacionais/Internet das Coisas (IoT) e servidores em ambientes virtuais, baseados em nuvem e físicos.
Ativos corporativos expostos externamente	Referem-se aos ativos corporativos que são públicos e podem ser descobertos por meio de reconhecimento do sistema de nomes de domínio e varredura de rede da Internet pública fora da rede da empresa.
Ativos corporativos internos	Referem-se a ativos corporativos não-públicos que só podem ser identificados por meio de varreduras de rede e reconhecimento de dentro da rede da empresa por meio de acesso autorizado autenticado ou não autenticado.
Biblioteca	Código pré-escrito, classes, procedimentos, scripts, dados de configuração e outros, usados para desenvolver programas de software e aplicações. É projetado para auxiliar o programador e o compilador da linguagem de programação na construção e execução do software.
Dispositivos móveis de usuário final	Pequenos dispositivos corporativos de usuário final com capacidade intrínseca sem fio, como smartphones e tablets. Dispositivos móveis de usuário final são um subconjunto de dispositivos portáteis de usuário final, incluindo laptops, que podem exigir hardware externo para conectividade. Para os fins deste documento, os dispositivos móveis de usuário final são um subconjunto dos dispositivos de usuário final.
Dispositivos de rede	Dispositivos eletrônicos necessários para comunicação e interação entre dispositivos em uma rede de computadores. Os dispositivos de rede incluem pontos de acesso sem fio, firewalls, gateways físicos/virtuais, roteadores e switches. Estes dispositivos consistem em hardware físico, bem como dispositivos virtuais e baseados em nuvem. Para os fins deste documento, os dispositivos de rede são um subconjunto dos ativos corporativos.
Infraestrutura de rede	Refere-se a todos os recursos de uma rede que tornam possível a conectividade, a gestão, as operações comerciais e a comunicação de rede ou Internet. Consiste em hardware e software, sistemas e dispositivos e permite a computação e a comunicação entre usuários, serviços, aplicações e processos. A infraestrutura de rede pode ser em nuvem, física ou virtual.
Dispositivos não computacionais/Internet das Coisas (IoT)	Dispositivos incorporados com sensores, software e outras tecnologias com a finalidade de conectar, armazenar e trocar dados com outros dispositivos e sistemas pela Internet. Embora esses dispositivos não sejam usados para processos computacionais, eles oferecem suporte à capacidade de uma empresa de conduzir processos de negócios. Exemplos destes dispositivos

	incluem impressoras, telas inteligentes, sensores de segurança física, sistemas de controle industrial e sensores de tecnologia da informação. Para os fins deste documento, os dispositivos não computacionais/IoT são um subconjunto dos ativos corporativos.
Sistema operacional	Software dos ativos corporativos que gerencia recursos de hardware e software do computador e fornece serviços comuns para programas. Os sistemas operacionais são considerados ativos de software e podem ser simples ou multitarefa, de um ou vários usuários, distribuídos, modelados, embarcados, em tempo real e bibliotecas.
Ambiente físico	Componentes físicos de hardware que constituem uma rede, incluindo cabos e roteadores. O hardware é necessário para comunicação e interação entre dispositivos em uma rede.
Dispositivos portáteis de usuário final	Dispositivos transportáveis de usuário final que têm a capacidade de se conectar a uma rede sem fio. Para os fins deste documento, dispositivos portáteis de usuário final podem incluir laptops e dispositivos móveis, como smartphones e tablets, todos os quais são um subconjunto de ativos corporativos.
Dispositivos remotos	Qualquer ativo corporativo capaz de se conectar a uma rede remotamente, geralmente da Internet pública. Isso pode incluir ativos corporativos, como dispositivos de usuário final, dispositivos de rede, dispositivos não computacionais/ Internet das Coisas (IoT) e servidores.
Sistemas de arquivos remotos	Permitem que uma aplicação executada em um ativo corporativo acesse arquivos armazenados em um ativo diferente. Os sistemas de arquivos remotos geralmente tornam outros recursos, como dispositivos remotos não computacionais, acessíveis a partir de um ativo. O acesso remoto ao arquivo ocorre por meio de alguma forma de rede local, rede de longa distância, link ponto a ponto ou outro mecanismo de comunicação. Esses sistemas de arquivos são frequentemente chamados de sistemas de arquivos de rede ou sistemas de arquivos distribuídos
Mídia removível	Qualquer tipo de dispositivo de armazenamento que pode ser removido de um computador enquanto o sistema está funcionando e permite que os dados sejam movidos de um sistema para outro. Exemplos de mídia removível incluem discos compactos (CDs), discos versáteis digitais (DVDs) e discos Blu-ray, backups em fita, bem como disquetes e unidades de barramento serial universal (USB).
Servidores	Um dispositivo ou sistema que fornece recursos, dados, serviços ou programas a outros dispositivos em uma rede local ou em uma rede remota. Os servidores podem fornecer recursos e usá-los de outro sistema ao mesmo tempo. Os exemplos incluem servidores web, servidores de aplicações, servidores de email e servidores de arquivos.
Contas de serviço	Uma conta dedicada com privilégios escalados usada para executar aplicações e outros processos. As contas de serviço também podem ser criadas apenas para possuir dados e arquivos de configuração. Elas não se destinam ao uso por pessoas, exceto para a execução de operações administrativas.
Serviços	Refere-se a uma funcionalidade de software ou um conjunto de funcionalidades de software, como a recuperação de informações especificadas ou a execução de um conjunto de operações. Os serviços fornecem um mecanismo para permitir o acesso a um ou mais recursos, onde o acesso é fornecido usando uma interface determinada e com base na identidade do solicitante de acordo com as políticas de uso da empresa.
Engenharia social	Refere-se a uma ampla gama de atividades maliciosas realizadas por meio de interações humanas em várias plataformas, como e-mail ou telefone. Depende de manipulação POSICcológica para induzir os usuários a cometer erros de segurança ou fornecer informações sensíveis.
Ativos de software	Também chamados de software neste documento, são os programas e outras informações operacionais usados em um ativo corporativo. Os ativos de software incluem sistemas operacionais e aplicações.
Contas de usuário	Uma identidade criada para uma pessoa em um computador ou sistema de computação. Para os fins deste documento, contas de usuário referem-se a contas de usuário “padrão” ou “interativas” com privilégios limitados e usadas para tarefas gerais, como ler e-mail e navegar na web. Contas de usuário com privilégios escalados são cobertas por contas de administrador.
Ambiente virtual	Simulação de hardware que permite que um ambiente de software seja executado sem a necessidade de usar hardware real. Ambientes virtualizados são usados para fazer com que um pequeno número de recursos atue como muitos, com bastante processamento, memória, armazenamento e capacidade de rede. A virtualização é uma tecnologia fundamental que permite que a computação em nuvem funcione.
PMU	Prefeitura Municipal da Estância Balneária de Ubatuba.
SMTI	Secretaria Municipal de Tecnologia da Informação
CSegInfo	Comitê de Segurança da Informação e Proteção de Dados
POSIC	Política de Segurança de Informação e Comunicação
SegCiber	Segurança Cibernética é um conjunto de processos, práticas recomendadas e soluções tecnológicas que ajudam a proteger seus sistemas críticos e sua rede contra ataques digitais.

INTRODUÇÃO

A Política de Segurança da Informação e Comunicação - POSIC define as diretrizes, os limites e o direcionamento que a Prefeitura Municipal de Ubatuba deseja para os controles que serão implantados na proteção de suas informações e a responsabilidade legal de todos os colaboradores e usuários, devendo ser cumprida e aplicada em todas as áreas da administração direta e indireta.

Esta POSIC tem como referência os guias de melhores práticas elaborados e em aplicação na Administração Pública Federal, disponibilizados pelo Departamento de Privacidade e Segurança da Informação da Secretaria de Governo Digital (DPOSIC/SGD) do Ministério da Economia.

Foram observadas também as recomendações propostas pela norma técnica nacional ABNT NBR ISO/IEC 27001:2006 e 27002:2005, código de prática para a gestão da segurança da informação, bem como está em conformidade com as leis vigentes em nosso país, e no *framework* "Controles CIS Versão8", mantido pela Center for Internet Security (CIS) que é uma organização internacional sem fins lucrativos, composta por corporações, agências governamentais e instituições acadêmicas.

Para efeito desta política de segurança, baseado na norma técnica ABNT NBR ISO/IEC 27001:2006, aplicam-se os seguintes termos e definições:

Ativo - qualquer coisa que tenha valor para a organização
Disponibilidade - propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada
Confidencialidade - propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados
Segurança da Informação - preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas
Evento de Segurança da Informação - uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação
Incidente de Segurança da Informação - um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação
Sistema de Gestão da Segurança da Informação SGSI - a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação (Nota: O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.)
Integridade - propriedade de salvaguarda da exatidão e completeza de ativos
Risco Residual - risco remanescente após o tratamento de riscos
Aceitação do Risco - decisão de aceitar um risco
Análise de Riscos - uso sistemático de informações para identificar fontes e estimar o risco
Análise/Avaliação de Riscos - processo completo de análise e avaliação de riscos
Avaliação de Riscos - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco
Gestão de Riscos - atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. (Nota: A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos)
Tratamento do Risco - processo de seleção e implementação de medidas para modificar um risco (Nota: Nesta Norma o termo "controle" é usado como um sinônimo para "medida")
Declaração de Aplicabilidade - declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI da organização

1. OBJETIVO

Este documento tem como objetivo definir o tratamento a ser dado às informações armazenadas, processadas ou transmitidas no ambiente de tecnologia da Prefeitura Municipal de Ubatuba, e estabelecer e definir normas, processos, procedimentos e controles específicos de segurança da informação, recursos e estruturas, bem como implementá-los.

Preservar as informações quanto à:

1.1. **Confidencialidade**: compreende a proteção de dados transmitidos contra ataques passivos, isto é, contra acessos não autorizados, envolvendo medidas como controle de acesso e criptografia. A perda da confidencialidade ocorre quando há uma quebra de sigilo de uma determinada informação (exemplo: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários;

1.2. **Autenticidade**: está preocupada em garantir que uma comunicação é autêntica, ou seja, origem e destino podem verificar a identidade da outra parte envolvida na comunicação, com o objetivo de confirmar que a outra parte é realmente quem alega ser. A origem e o destino tipicamente são usuários, dispositivos ou processos.

1.3. **Integridade**: A integridade pode ser considerada sob dois aspectos: serviço sem recuperação ou com recuperação. A perda de integridade surge quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário da informação.

1.4. **Não repúdio**: compreende a capacidade que previne uma origem ou destino de negar a transmissão de mensagens, isto é, quando dada mensagem é enviada, o destino pode provar que esta foi realmente enviada por determinada origem, e vice-versa.

1.5. **Conformidade**: dever de cumprir e fazer cumprir regulamentos internos e externos impostos às atividades da organização. Estar em conformidade é estar de acordo, seguindo e fazendo cumprir leis e regulamentos internos e externos.

1.6. **Controle de acesso**: trata de limitar e controlar o acesso lógico/físico aos ativos de uma organização por meio dos processos de identificação, autenticação e autorização, com o objetivo de proteger os recursos contra acessos não autorizados.

1.7. **Disponibilidade**: determina que recursos estejam disponíveis para acesso por entidades autorizadas, sempre que solicitados, representando a proteção contra perdas ou degradações. A perda de disponibilidade acontece quando a informação deixa de estar acessível por quem necessita dela.

2. PRINCÍPIOS

2.1. Toda informação, produzida ou recebida pelos usuários como resultado da atividade profissional, pertence à Prefeitura Municipal de Ubatuba.

2.2. Todos os equipamentos, sistemas e informações devem ser utilizados pelos usuários para a realização das atividades profissionais. O uso deles com finalidade pessoal é proibido.

2.3. Esta POSIC dá ciência a cada usuário que os ambientes, sistemas, dispositivos informáticos e redes, no âmbito da administração direta e indireta, serão monitorados e gravados, conforme previsto nas leis brasileiras.

3. ABRANGÊNCIA

3.1. As diretrizes aqui estabelecidas deverão ser seguidas por todos os usuários que utilizam sistemas e recursos de Tecnologia da Informação e Comunicação da PMU.

3.2. Os usuários não pertencentes ao quadro de funcionários da PMU, estão sujeitos às regras estabelecidas neste documento ao utilizarem os sistemas e recursos da PMU.

4. ESTRUTURAÇÃO NORMATIVA

As tratativas de Segurança da Informação e Comunicação serão estabelecidas através dos seguintes artefatos:

4.1. Política de Segurança da Informação e Comunicação - POSIC (**POLÍTICA**): constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação.
4.2. Plano (**PLANOS**): é um documento utilizado para fazer um planejamento de trabalho necessário referente a um objetivo específico, para atingimento de um resultado desejado ou na resolução de problemas ou uma necessidade.
4.3. Normatização (**NORMAS**): estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;
4.4. Procedimentos de Segurança da Informação (**PROCEDIMENTOS**): instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da Prefeitura Municipal de Ubatuba.

5. FORMULAÇÃO E REVISÃO

Os documentos integrantes da estrutura normativa da Segurança da Informação e Comunicação da Prefeitura Municipal de Ubatuba serão aprovados e revisados quando motivados por algum fato relevante ou evento, e conforme os seguintes critérios:

5.1. **Política**
- Nível de Aprovação: Alta Gestão e CSegInfo
- Periodicidade de Revisão: anual

5.2. **Normas**
- Nível de Aprovação: - SMTI e CSegInfo
- Periodicidade de Revisão: anual

5.3. **Procedimentos**
- Nível de Aprovação: SMTI
- Periodicidade de Revisão: a qualquer tempo

6. SEGURANÇA EM RECURSOS HUMANOS

A segurança dos recursos e o uso dos componentes da Tecnologia da Informação e Comunicação é tema que vai além dos limites da área de tecnologia. São necessários o comprometimento e a vigilância das diversas áreas da administração municipal, cuidando para correta e segura utilização dos meios, visando combater o uso e acesso indevido dos recursos e informações.

A Política e as Normas de Segurança da Informação e Comunicação deverão ser divulgadas a todos os usuários e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento, utilizando os diversos canais disponíveis.

6.1. Visando a correta orientação, os servidores ou prestadores de serviço que utilizem os recursos de Tecnologia da Informação e Comunicação devem:

6.1.1. Tomar conhecimento formal das políticas, normas e procedimentos;

6.1.2. Serem conscientizados e entender suas responsabilidades;

6.1.3. Serem orientados sobre as boas práticas.

Convém que a as chefias orientem e solicitem aos servidores ou prestadores de serviço, sob sua responsabilidade, que observem as boas práticas de segurança e obedeçam à política, normas e procedimentos.

7. PAPÉIS E RESPONSABILIDADES

Visa estabelecer estruturação dos atores e suas responsabilidades dentro dos mecanismos instrucionais e normativos que irão orientar os usos, procedimentos e controles específicos de segurança da informação e comunicação, bem como implementá-los. Define a cadeia organizacional e seus papéis:

7.1. **Papéis**

Papel	**Perfil Associado**	**Descrição**
Usuário Interno	Servidores públicos do quadro permanentes ou não	Todos os servidores, gestores, técnicos, estagiários, bolsistas de programas educacionais, que fazem uso dos recursos informacionais e computacionais da PMU.
Usuário Externo	Prestadores de serviço e demais colaboradores externos	Prestadores de serviços contratados direta ou indiretamente pela PMU e demais colaboradores externos que fazem uso de seus recursos informacionais e computacionais.
Gestores	Todos os cargos de chefia da PMU	Todos aqueles que exercem funções de gerência no âmbito da organização, administrando pessoas e/ou processos.
SMTI	Integrantes da Secretaria Municipal de Tecnologia da Informação	Gestor de Segurança da Informação e Comunicação na PMU.
CSegInfo	Comitê permanente intersetorial	Propor, acompanhar e revisar a Política e Normas de Segurança da Informação na PMU, em conformidade com a legislação existente sobre o tema
Alta Gestão	Prefeito(a), Chefia de Gabinete e Secretaria de Governo	Aprovar as proposições do CSegInfo e acompanhar a execução.

7.2. **Responsabilidades**

7.2.1. São **RESPONSABILIDADES GERAIS** e comuns a todos que utilizarem os serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos de informação e comunicação da PMU:

a) Zelar pela segurança de suas contas de acesso;

b) Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos corporativos de informação e comunicação – utilizando-os sempre de forma ética, legal e consciente;
c) Manter-se atualizado em relação a esta POSIC e às suas normas complementares e procedimentos relacionados.

7.2.2. São **RESPONSABILIDADES ESPECÍFICAS** aos usuários que utilizarem os serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos de informação e comunicação da PMU, conforme seus papéis:

7.2.2.1. **Usuários Interno e Externos**

a) Entende-se por **USUÁRIO** toda e qualquer pessoa física, servidor concursado ou comissionado, ou prestador de serviço como pessoa física ou por intermédio de pessoa jurídica, que exerça alguma atividade relacionada à PMU;
b) A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento;
c) Será de inteira responsabilidade de cada usuário, todo prejuízo ou dano que vier a sofrer ou causar à Prefeitura Municipal de Ubatuba ou à terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas;
d) Os usuários são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, login, senha, assinatura eletrônica, certificado digital e endereço de correio eletrônico;
e) Comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à SMTI ou ao responsável pela unidade administrativa.

7.2.2.2. **Gestores**

a) Entende-se como **GESTOR** todo aquele que se encontrar em posição de chefia de unidade administrativa e tiver usuários sob sua responsabilidade, cabendo a ele:
b) Conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de Segurança da Informação e Comunicação;
c) Incorporar aos processos de trabalho de sua unidade, práticas inerentes à Segurança da Informação e Comunicação;
d) Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da Segurança da Informação e Comunicação por parte dos usuários sob sua supervisão;
e) Comunicar à SMTI os casos de quebra de segurança.

7.2.2.3. **SMTI**

a) A **SMTI** é a secretaria responsável pela gerência e a operação da atividade de Tecnologia da Informação e Segurança da Informação e Comunicação na PMU, cabendo a ela:
b) Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;
c) Promover a recuperação de sistemas em casos de falhas;
d) Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de segurança da informação e avaliando condições de segurança de redes por meio de verificações de conformidade;

e) Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
f) Analisar ataques e intrusões na rede da PMU;
g) Executar as ações necessárias para tratar quebras de segurança;
h) Cooperar com outras equipes de Tratamento e Resposta a Incidentes;
i) Participar em fóruns, redes nacionais e internacionais relativas à Segurança da Informação;
j) Formular e propor procedimentos e normas.

7.2.2.4. **CSegInfo**

a) O Comitê De Segurança Da Informação E Proteção De Dados – **CSegInfo** é um órgão permanente com o objetivo de desenvolver e monitorar políticas e diretrizes estratégicas transversais relativas à governança de tecnologia da informação e comunicação e à segurança da informação, cabendo a ele:
b) elaborar e implementar, propostas de normas e políticas de proteção de dados - POSIC;
c) efetuar revisão periódicas anuais das Política de Segurança da Informação e normas relacionadas e sugerir alterações;
d) estabelecer diretrizes e definições estratégicas para as ações e projetos relacionados à Segurança da Informação;
e) dirimir dúvidas e deliberar sobre questões não contempladas na Política de Segurança da Informação e em normas relacionadas;
f) propor e acompanhar planos de ação para aplicação da Política de Segurança da Informação, assim como campanhas de conscientização dos usuários;
g) receber comunicações de descumprimento das normas referentes à Política de Segurança da Informação, instruí-las com os elementos necessários à sua análise e apresentar parecer à autoridade competente a apreciá-las;
h) solicitar à SMTI, quando necessário, a realização de auditorias extraordinárias, relativamente ao uso dos recursos de tecnologia da informação;
i) avaliar relatórios e resultados de auditorias apresentados pela SMTI;

j) apresentar ao Gabinete do Prefeito os resultados da aplicação das POSIC.

7.2.2.5. **Alta Gestão**

a) A **Alta Gestão** é integrada pelo(a) Prefeito(a) Municipal, Chefia de Gabinete e Chefia de Governo e é a última instancia da autoridade de governança da PMU, cabendo:
b) Comprometer-se com a segurança de informação da Administração Municipal;
c) Oficializar a POSIC e cobrar sua aplicação;
d) Garantir a provisão dos recursos necessários para a implementação da POSIC;
e) Cobrar o comprometimento de toda a organização administrativa com a POSIC;

8. DIRETRIZES GERAIS

Estabelecemos um conjunto de regras gerais que direcionam os tópicos principais da segurança da informação e que são suportadas por normas e procedimentos, orientando a segurança da informação,

conforme a necessidades, legislação e normas vigentes, podendo ser revistas e ampliadas à qualquer momento, ou nos períodos de revisão estabelecidos.

8.1. **Tratamento de Dados e Informação**

As diretrizes específicas e os procedimentos próprios de tratamento de dados e informação corporativos serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

8.1.1. Documentos corporativos imprescindíveis às atividades dos usuários deverão ser salvos em dispositivos de rede. Os arquivos gravados localmente, nos computadores dos usuários, não serão cobertos pelo serviço de backup (cópias de segurança) estando sujeitos a perda e a não-recuperação;

8.1.2. Arquivos pessoais e/ou não pertinentes às atividades laborais do usuário (fotos, músicas, vídeos, etc.) não deverão ser armazenados em ativos corporativos. Caso identificados, esses arquivos serão excluídos de forma imediata e definitiva sem necessidade de comunicação prévia ao usuário.

8.1.3. A classificação de informações (de uso públicas, compartilháveis, internos, confidencial e secreta) seus níveis de acesso, uso e descarte de ativos de informação, dentre outros temas afins, serão fixadas em estrita aderência às leis e normas atinentes à Administração Municipal, considerando as competências regimentais.

8.2. **Controle de Acessos e Recursos**

Diretrizes específicas e procedimentos próprios de controle de acessos físico e lógico aos recursos. Serão regulamentados em **NORMA** complementar considerando as seguintes diretrizes gerais:

8.2.1. Como condição imprescindível à concessão de acessos aos ativos de informação, o usuário deverá firmar termo de compromisso de ciência das normas gerais de segurança da informação e comunicação contidas nesta política.

8.2.2. O controle de acesso deverá observar, na configuração das contas e concessão de credenciais de acesso o princípio do menor privilégio, que define que pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

8.2.3. A criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário. Para o usuário que não exerce funções de administração de rede será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

8.2.4. Os gestores, administradores e operadores dos recursos computacionais poderão, pela característica de suas credenciais (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários – observadas as restrições quanto ao acesso à informações invioláveis e mediante estrita necessidade do serviço.

8.2.5. O acesso à rede corporativa deve ocorrer de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em norma específica.

8.2.6. As práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança.

8.2.7. A política de uso detalhada será estabelecida através de **NORMA** definida pela SMTI, aprovada pela CSegInfo, com revisão anual, e obrigatoriedade e ciência a todos os **USUÁRIOS.**

8.3. **Sistemas de Comunicação e Mensagens**

Diretrizes específicas e procedimentos próprios ao serviço de sistemas de comunicação e mensagens corporativo (e-mail, aplicativos, workgroup) serão regulamentados em **NORMA** complementar considerando as seguintes diretrizes gerais:

8.3.1. Os sistemas corporativos de comunicação e mensagens são ferramentas para comunicação de trabalho no âmbito da PMU.
8.3.2. Os sistemas corpoativos de comunicação e mensagens são destinados para uso exclusivo em serviço e relacionado estritamente às atividades profissionais do usuário no âmbito da Administração Municipal.
8.3.3. Os sistemas corporativos de comunicação e mensagens podem ser monitorados a qualquer tempo pela SMTI, não cabendo ao usuário do serviço alegar ofensa ao sigilo das comunicações telemáticas.

8.4. **Treinamento e Conscientização**

A conscientização e o treinamento deverão ser ações contínuas, visando incorporar no usuário as noções de segurança e a importância de seu comportamento dentro do tema de Segurança da Informação e Comunicação da PMU:

8.4.1. Assegurar a existência de um programa de treinamento e conscientização em Segurança da Informação, Comunicação e Privacidade de Dados para todos os usuários, sendo que o mesmo deve ser tratado como procedimento obrigatório.
8.4.2. Contemplar em seu programa de treinamento e conscientização de segurança e privacidade de dados algumas campanhas com temas como phishing, orientação sobre engenharia social, palestras externas, boletins, informativos.
8.4.3. Os usuários que acessarem ou processarem dados pessoais e/ou informações sensíveis devem ter ciência desta Política e do que diz respeito a treinamento de segurança da informação e comunicação;

8.5. **Serviço de Backup e Restore**

Os procedimentos próprios ao serviço de Backup (cópia de segurança) e Restore (restauração de cópia de segurança) serão regulamentados em **PLANO** complementar, considerando as seguintes diretrizes gerais:

8.5.1. O serviço de backup deve ser preferencialmente automatizado por sistemas informacionais próprios considerando, inclusive, a execução agendada fora do horário de expediente normal do órgão, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.
8.5.2. A solução de backup deverá ser mantida atualizada, considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros).
8.5.3. A administração de mídias de backup deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter sua segurança e integridade.
8.5.4. Os backups críticos para o bom funcionamento dos serviços do PMU exigem uma regra de retenção especial, a ser prevista nos procedimentos específicos e de acordo com as

normas de classificação da informação pública, seguindo ainda as determinações fiscais e legais existentes no país.

8.5.5. A execução de rotinas de Backup e Restore deverá ser rigidamente controlada, documentada e auditada, nos termos do **PLANO** e procedimentos próprios.

8.6. **Conformidade dos Sistemas**

Visando a necessidade de atender aos requisitos da POSIC para Segurança da Informação, a Conformidade tem como objetivo, estabelecer padrões para o segmento de Sistemas de Informação e Comunicação. Aplicados a sistemas com desenvolvimento interno ou fornecimento de terceiros, devem:

8.6.1. No desenvolvimento interno:

- Desenvolver levando em consideração os padrões de legalidade, privacidade (no âmbito da Lei Geral de Proteção de Dados) e segurança aceitos pelo mercado (ex: CIS Controls 16, NIST Secure Software Development Framework, Microsoft SDL);
- Descrever os componentes e recursos de segurança e os dados acessados pelas aplicações, os quais devem ser avaliados pela área de Segurança de Informação durante a fase de homologação (ex: descritivo técnico da aplicação)
- e/ou Diagrama Funcional);
- Utilizar rotinas de validação de integridade para prevenir erros, seja involuntário ou intencional, utilizando de dados fictícios ou anonimizações e em ambiente não produtivo;
- Realizar análise de segurança no código-fonte;
- Realizar análise de segurança em suas aplicações (EHT e testes de intrusão);

8.6.2. Nas soluções de terceiros:

- Dispor de conformidade com os termos da POSIC para homologação;

8.7. **Gestão do Data Center**

Os procedimentos para administração do centro de processamento de dados (data center) serão regulamentados em norma complementar considerando as seguintes diretrizes gerais:

8.7.1. A administração de dados e de serviços de data center é tarefa tecnicamente complexa cuja gestão é competência exclusiva da SMTI.

8.7.2. O acesso físico ao data center deverá ser feito por sistema de autenticação pessoal, mediante uso de solução adequada. O acesso físico por meio de chave apenas poderá ocorrer em situações de emergência, quando a segurança física do data center estiver comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

8.7.3. O acesso ao data center por visitantes ou terceiros somente poderá ser realizado com acompanhamento de um servidor autorizado, com finalidade pertinente.

8.7.4. A lista de usuários com direito de acesso ao data center deverá ser documentada e constantemente atualizada. Ocorrendo o desligamento de usuários que possuam acesso ao data center, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de usuários autorizados.

8.7.5. A função de administrador do data center – incluindo seu sistema de autenticação forte – deverá ser atribuída exclusivamente a servidor público efetivo, integrante do quadro de pessoal da SMTI.

8.8. **Monitoramento e Auditoria do Ambiente**

Para garantir a aplicação das diretrizes mencionadas nesta POSIC, além de fixar normas e procedimentos complementares sobre o tema, o PMU poderá:

8.8.1. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
8.8.2. Disponibilizar informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do CSegInfo;
8.8.3. Realizar, a qualquer tempo e sem prévio aviso, inspeções físicas nos equipamentos e instalações de sua propriedade;
8.8.4. Instalar sistemas de proteção, preventivos e detectáveis, para garantir segurança das informações, capacidade de detecção e resposta a software maliciosos (vírus, trojan malware, spyware, entre outros) e dos perímetros de acesso;
8.8.5. Desinstalar, a qualquer tempo e sem prévio aviso, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

8.9. **Acesso e uso da Internet**

Diretrizes específicas e procedimentos próprios de controles de uso e acesso à Internet serão regulamentados em **NORMA** complementar considerando as seguintes diretrizes gerais:

8.9.1. Todas as regras corporativas sobre uso de Internet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação do PMU deverá sempre ser privilegiada.
8.9.2. Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, a PMU, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à rede mundial de computadores.
8.9.3. Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, caixa postal de correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando a assegurar o cumprimento de sua Política de Segurança da Informação e Comunicações.
8.9.4. Os equipamentos particulares, que autorizados para uso dentro da PMU, obrigatoriamente obedecem ao estabelecido nesta POSIC;

8.10. **Assinatura Eletrônica e Digital**

A assinatura eletrônica é um recurso regulamentado em nível nacional com destaque para a Medida Provisória nº 2.200-2, de 24 de agosto de 2001, e Lei Federal nº 14.063, de 23 de setembro

de 2020. Sua utilização tem validade legal instituída, com normatização municipal específica, e que terá seu uso permitido através de termo de responsabilidade de uso, considerando:

8.10.1. **Assinatura Eletrônica Simples**, que é qualquer forma de identificação eletrônica que pode ser confirmada por um conjunto de dados e evidências digitais como codificação em metadados e-mail, registro de Geolocalização, biometria, áudio, foto ou vídeo, registro de endereço IP ou identificação da conexão, código de SMS, entre outros. A Assinatura Eletrônica não exige certificação digital de entidade validadora;

8.10.2. **Assinatura Eletrônica Avançada**, é um tipo de assinatura eletrônica superior a Assinatura Eletrônica Simples, dispondo de meio de comprovação da autoria e da integridade de documentos em forma eletrônica;

8.10.3. **Assinatura Digital Qualificada**, é um tipo de assinatura eletrônica. Ela é realizada por meio de um certificado digital, no padrão da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) regulada pelo Instituto Nacional de Tecnologia da Informação (ITI), onde é necessário adquirir um certificado digital, emitido por uma Autoridade Certificadora, e ele possui uma chave criptográfica única, que ajuda a identificar o signatário;

8.11. Gestão de Riscos de Segurança de Informação e Comunicação

A "Gestão de Riscos de Segurança da Informação e Comunicações é o conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos". As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicações do PMU deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão, direta e indireta, além de estarem alinhadas a esta Política de Segurança da Informação e Comunicações. Esse processo deverá ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações, contemplando inclusive as contratações de soluções de TI – para as quais deverá ser elaborado um Plano de Tratamento de Riscos.

8.12. Gestão de Continuidade

A implantação de **PLANO** que busque minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação. A PMU deverá elaborar e manter o PCN - Plano de Continuidade de Negócios, aqui entendido como o "processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção". O Programa de Gestão de Continuidade de Negócios do PMU deverá ser composto, no mínimo, pelos seguintes Planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos ativos de informação e a recuperação das atividades críticas:

8.12.1. **Plano de Gerenciamento de Incidentes de Segurança da Informação:** plano de ação claramente definido e documentado, a ser usado quando ocorrer um incidente, abrangendo as principais pessoas, recursos, serviços e ações necessárias para implementar o processo de gerenciamento de incidentes.

8.12.2. **Plano de Continuidade de TIC:** documentação dos procedimentos e informações necessárias para que o PMU mantenha seus ativos de informação críticos e a continuidade de suas atividades críticas de TIC, num nível previamente definido, em casos de incidentes.

8.12.3.

8.13. **Tratamento de Incidentes em Redes Computacionais**

O tratamento de Incidentes de Segurança em Redes Computacionais é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências". A ocorrência de incidentes de segurança em redes de computadores da PMU deverá ser comunicada a SMTI, responsável pelo tratamento e resposta ao incidente, deverá considerar, no mínimo, as seguintes diretrizes:

8.13.1. Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas.

8.13.2. O tratamento da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

8.13.3. Durante o gerenciamento de incidentes de segurança em redes computacionais, havendo indícios de ilícitos criminais, a SMTI tem como dever, sem prejuízo de suas demais atribuições, acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços da PMU.

9. PENALIDADES

Ações que violem a POSIC ou quebrem os controles de Segurança da Informação e Comunicações serão passíveis de sanções administrativas, civis e penais, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente, sendo:

9.1. O não cumprimento da POSIC, suas normas e regulamentos, por qualquer pessoa ou sistema, acarreta riscos à segurança da informação, cabendo à SMTI e a CSegInfo avaliar a necessidade de executar ação investigativa apropriada;

9.2. Processo disciplinar específico, quando couber, deverá ser instaurado para apurar formalmente as ações que constituem a quebra das diretrizes impostas por esta POSIC.

9.3. As violações /transgressões omissas nas legislações correlatas serão resolvidas pelo Comitê de Segurança da Informação e Comunicações.

9.4. As faltas listadas abaixo serão tratadas com agravante:

9.4.1.Uso de mecanismos para driblar os sistemas de monitoramento e controle utilizados;

9.4.2.Contaminar ou deixar-se contaminar de forma intencional por algum tipo de "Malware".

9.5. As punições serão efetivadas por meio de processo administrativo próprio e tratadas como dano ao patrimônio público, sem prejuízo da responsabilidade civil e criminal.

9.6. São exemplos de crimes definidos na legislação:
- 9.6.1. Invasão de dispositivo informático (Lei 12.737, Art. 2º - detenção de 3 meses a 1 ano);
- 9.6.2. Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (Lei 12.737, Art. 3º - detenção de 1 a 3 anos);
- 9.6.3. Divulgação de segredo (Lei 9.983, Art. 2º - detenção de 1 a 4 anos);
- 9.6.4. Inserção de dados falsos em sistemas de informações (Lei 9.983, Art. 1º - reclusão de 2 a 12 anos);
- 9.6.5. Modificação ou alteração não autorizada de sistema de informações (Lei 9.983, Art. 1º - detenção, de 3 meses a 2 anos, + ⅓ se dano para Administração Pública);
- 9.6.6. Dano qualificado (inclui destruição de informação) (Lei 5.346 - detenção de 6 meses a 3 anos)

10. CONTROLES DE SEGURANÇA

A maior referência em boas práticas utilizada mundialmente é a versão 8 do framework do Center for Internet Security (CIS), organização independente e sem fins lucrativos que recomenda um total de 18 controles críticos de SegCiber, os quais formam um conjunto de ações de defesa de alta prioridade contra-ataques cibernéticos mais pervasivos. São ações consideradas imprescindíveis e urgentes para toda organização que busca melhorar a própria SegCiber, sendo formalmente recomendação de órgão de controle como o TCU e adotado por diversos órgãos em nível nacional.

A aplicação dos controles do CIS consiste em um importante passo de um processo para orientar o programa de melhoria de segurança da PMU, sendo importante destacar que o documento não se trata de “somente uma lista" de boas práticas que podem ajudar na segurança da instituição, e sim de um documento confiável com recomendações de segurança e suporte de uma comunidade de especialista para tornar os controles implementáveis, utilizáveis, escaláveis e alinhados com todos os requisitos de segurança da indústria ou do governo.

Sendo composto por grupos de controles específicos, os Controles CIS são orientações prescritivas e podem ser aplicadas no todo ou em grupos selecionados.

Sendo um documento orientador, o documento “Controles CIS Versão 8” é organizado em um conjunto prioritário e prescritivo de práticas recomendadas de segurança cibernética e ações defensivas que podem ajudar a prevenir os ataques mais generalizados e perigosos, dando suporte à conformidade em uma era de múltiplas estruturas, sendo:

- Controle 1 - Inventário e controle de ativos corporativos
- Controle 2 - Inventário e controle de ativos de software
- Controle 3 - Proteção de dados
- Controle 4 - Configuração segura de ativos corporativos e software
- Controle 5 - Gestão de contas
- Controle 6 - Gestão de controles de acesso
- Controle 7 - Gestão contínua de vulnerabilidades
- Controle 8 - Gestão de registros (logs) de auditoria
- Controle 9 - Proteção de e-mail e navegador da web
- Controle 10 - Defesa contra malware
- Controle 11 - Recuperação de dados
- Controle 12 - Gestão de infraestrutura de rede
- Controle 13 - Monitoramento e defesa de rede
- Controle 14 - Conscientização sobre segurança e treinamento de competências
- Controle 15 - Gestão de provedores de serviço
- Controle 16 - Segurança de aplicações de software
- Controle 17 - Gestão de respostas a incidentes
- Controle 18 - Teste de invasão

Pela maturidade, aplicação e larga aceitação, o framework Controles CIS Versão 8, será adotado como orientador nas ações de segurança da PMU.

11. CONCLUSÃO

Concluímos os trabalhos de elaboração da Política de Segurança da Informação e Comunicação - POSIC da Prefeitura Municipal de Ubatuba, que será decretada e publicada.

O documento foi aprovado em reunião técnica do Comitê de Segurança da Informação e Proteção de Dados – CSegInfo na Reunião nº 01, de 16 de dezembro de 2022.

Todos os atos referentes a POSIC estão registrados no processo administrativo SA/14.715/2022.

12. DOCUMENTOS DE REFERÊNCIA

- **"Controles CIS v8" - www.cisecurity.org/controls**
- **"Guia do Framework de Segurança" - www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_framework_seguranca.pdf**
- **Gestão da Segurança da Informação NBR 27001 e NBR 27002 - https://esr.rnp.br/cursos/gestao-da-seguranca-da-informacao-nbr-27001-e-nbr-27002-presencial-gti8/**
- **Índice de Efetividade da Gestão Municipal TCE/SP - www.tce.sp.gov.br/sites/default/files/publicacoes/Manual-IEGM%202022%20-%20Ano%20Base%202021.pdf**