mesmo em seu nome, deverá firmar a Declaração de Posse/ Responsável Tributário.

Art. 17. O contribuinte, seu representante legal ou o procurador com poderes especiais deverá, no ato de formalização do requerimento, apontar quais débitos deseja pagar e seu valor.

§ 1º O contribuinte deverá, ainda, assinar confissão de dívida, reconhecendo os débitos incluídos no pedido.

§ 2º O termo de confissão de dívida conterá cláusulas que disciplinarão:

I- caso os débitos estejam, parcial ou integralmente, sendo discutidos na via administrativa, a desistência a impugnações, reclamações ou recursos já interpostos em face dos mesmos, ou a serem interpostos em momento futuro;

II- renúncia ao direito sobre o qual se funda ações que versem sobre o crédito municipal aderido ao programa, casos os débitos já tenham sido judicializados, com consequente renúncia a Embargos do devedor, Exceções de Pré-Executividade ou eventuais recursos inerentes, bem como ao direito a verbas sucumbências eventualmente devidas pelo município.

§ 3º A Secretaria Municipal de Fazenda procederá à juntada do referido Termo nos processos administrativos e a Procuradoria Fazendária nos processos judiciais, conforme o caso atendendo ao que trata o parágrafo anterior.

Art. 18. A fim de aproveitar os dados trazidos pelos próprios contribuintes, a Secretaria Municipal de Fazenda promoverá atualização cadastral no sistema informatizado do município de todos os processos do REFIS/RO, por setor específico com as respectivas Gerências Cadastrais.

Art. 19. O contribuinte que aderir ao REFIS/RO, fica impedido de realizar nova adesão ao referido programa, bem como à anistia e congêneres, num prazo inferior a 02 (dois) anos.

Art. 20. O Programa REFIS/RO terá a duração conforme previsão legal do artigo 2º desta Lei, podendo ser prorrogado uma única vez por até 30 (trinta) dias, por ato do Poder Executivo.

Art. 21. Esta Lei poderá ser regulamentada por ato do Chefe do Poder Executivo, de modo a otimizar e disciplinar sua operacionalização.

Art. 22. Esta Lei entra em vigor na data de sua publicação.

Rio das Ostras, 07 de junho de 2023.

MARCELINO CARLOS DIAS BORBA
Prefeito do Município de Rio das Ostras

DECISÃO

Processo Administrativo nº 33470/2022
APLICO à empresa ENGECORP MANUTENÇÃO E SERVIÇOS LTDA, antiga RELUZ EMPREENDIMENTOS E SERVIÇOS LTDA, CNPJ nº 10.471.095/0001-85, a penalidade de multa no valor de R$ 13.849,33 (treze mil, oitocentos e quarenta e nove reais e trinta e três centavos), correspondente a 3% sobre o valor de referência para licitação, com fundamento no art. 7º, inciso V, alínea “d” do Decreto nº 2092/2019, cumulado com a suspensão temporária de participação em licitação e do impedimento de contratar com o Município de Rio das Ostras, pelo período de 24 (vinte e quatro) meses, com fundamento no art. 12, inciso III, alínea “b”, do Decreto nº 2092/2019.

Rio das Ostras, 07 de junho de 2023

MARCELINO CARLOS DIAS BORBA
Prefeito do Município de Rio das Ostras

DECRETO Nº 3622/2023

ATUALIZA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO-PSI NO MUNICÍPIO DE RIO DAS OSTRAS, APROVADA ANTERIORMENTE POR MEIO DO DECRETO Nº 2.111, DE 08 DE MARÇO DE 2019.

O PREFEITO DO MUNICÍPIO DE RIO DAS OSTRAS, Estado do Rio de Janeiro, no uso de suas atribuições legais, em consonância ao Processo Administrativo nº 21939/2023,

DECRETA:

Art. 1º Fica atualizada a Política de Segurança da Informação-PSI, no âmbito do Município de Rio das Ostras, nos termos do Anexo Único deste Decreto.

Art. 2º Este decreto entrará em vigor na data de sua publicação.

Rio das Ostras, 07 de junho de 2023.

MARCELINO CARLOS DIAS BORBA
Prefeito do Município de Rio das Ostras

ANEXO ÚNICO DO DECRETO Nº 3622/2023

Prefeitura Municipal de Rio das Ostras
PSI – Política de Segurança da Informação
Documento de Diretrizes e Normas Administrativas
Responsáveis pelo documento:

	Nome	Matrícula	Cargo
Elaboração	Stefan Augusto Beloti Pizetta	11243-7	Analista de Segurança
Revisão	Adalberto Pires de Oliveira	4688-4	Técnico de Informática
	Alessandro de Oliveira Rodrigues	10814-6	Agente Administrativo
Aprovação	Luiz Paulo Jorge Duarte	18776-3	Coordenador de Tecnologia da Informação
	Cintia Moreira de Castro	18741-5	Assessora de Comunicação Social e Tecnologia da Informação

SUMÁRIO

POLÍTICA DE SEGURANÇA DE TI

APRESENTAÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Prefeitura Municipal de Rio das Ostras para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2022, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

OBJETIVO

Garantir que os RECURSOS COMPUTACIONAIS e SERVIÇOS DE TI serão utilizados de maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando exposição que possa prejudicar a PMRO, colaboradores e terceiros.

A Política deve implementar controles para preservar os interesses da PMRO contra danos que possam acontecer devido a falha de segurança. Ela deve descrever as normas de utilização e possíveis atividades que possam ser consideradas como violação ao uso dos serviços e, portanto, considerados proibidos.
Preservar as informações da PMRO quanto à:
• Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
• Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
• Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
As normas descritas no decorrer devem sofrer alterações sempre que necessário, sendo que estas devem ser registradas pela equipe de TI, aprovadas pela comissão de TI e divulgadas pela COTINF - ASCOMTI, dentro da estrutura de processo organizacional da Divisão de Infraestrutura de Dados, DINF - COTINF(ANEXO I), considerando-se o tempo hábil para que eventuais providências sejam tomadas.
Tais normas são fornecidas, a título de orientação aos usuários. Em caso de dúvida o usuário deverá procurar Divisão de Suporte Técnico, DIST – CONTIF, para maiores esclarecimentos.
Caso os procedimentos ou normas aqui estabelecidos sejam violados por usuários, a CONTIF - ASCOMTI informará aos órgãos competentes de forma que sejam tomadas as medidas cabíveis.

Esta política aplica-se a todos os usuários dos recursos computacionais e serviços de TI da PMRO.

DEFINIÇÕES:

PMRO - Prefeitura Municipal de Rio das Ostras.
TI - Tecnologia da Informação, pode-se definir como o conjunto de todas as atividades e soluções providas por recursos de computação que visam a produção, o armazenamento, a transmissão, o acesso, a segurança e o uso das informações.
COTINF - Coordenadoria de Tecnologia da Informação.
DIST - Divisão de Suporte Técnico.
DINF - Divisão de Infraestrutura de Dados.
ASCOMTI – Assessoria de Comunicação Social e Tecnologia da Informação.
USUÁRIOS - Toda e qualquer pessoa, seja física ou jurídica, que venha utilizar os recursos computacionais e serviços de TI da PMRO. Também considerados FUNCIONÁRIOS/COLABORADORES.
RECURSOS COMPUTACIONAIS - são ativos de tecnologia da informação, administrados, mantidos ou operados pela PMRO, tais como:
Computadores e terminais de qualquer espécie, incluídos seus acessórios;
Periféricos e afins;
Redes de computadores e de transmissão de dados e seus acessórios;
Dispositivos de segurança e sistemas de energia elétrica;
Discos, mídias, fitas e meios de armazenamentos;
Bancos de dados ou informações ou documentos residentes em disco, mídia, fita ou outros meios de armazenamentos;
Ambientes informatizados;
Serviços e informações disponibilizados via a arquitetura de informática da instituição;
Softwares e hardwares adquiridos ou desenvolvidos.
SERVIÇOS DE TI - de acordo com o ITIL, “é um serviço provido para um ou mais clientes por um provedor de serviços, que suporta os processos de negócios deste (s) cliente (s), é feito de uma combinação de pessoas, processos e tecnologia e deve ser definido por acordos de nível de serviço”.

POLÍTICA DE SEGURANÇA DA ESTRUTURA DE INFORMÁTICA
Abrange itens relacionados a utilização desta estrutura, como política de utilização da rede, utilização e administração de contas, senhas, correio eletrônico, acesso à Internet, uso das estações de trabalho, utilização de impressoras, etc.

1. POLÍTICA DE UTILIZAÇÃO DA REDE
1.1. Disposições gerais

Esta Resolução Normativa define as normas relativas ao controle do acesso lógico aos ativos de tecnologia da informação da PMRO e não abrange o controle de acesso físico aos ativos de tecnologia da informação.
Se aplica a todos os usuários de serviços de tecnologia da informação institucionais, tais como: servidores do quadro permanente, comissionados, cedidos, requisitados, terceirizados, discentes, estagiários, prestadores de serviços, usuário de unidade/setor e pessoal de associação temporária que usam serviços de tecnologia da informação da PMRO com acesso restrito, ou acesso autenticado.
Tem o objetivo de estabelecer normas para minimizar riscos à gestão de credenciais de acesso lógico, tendo como objetivos específicos:

I- especificar um modelo mínimo de controle de acesso lógico para proteger os ativos de tecnologia da informação de acessos não autorizados;
II- legitimar o processo de definição de responsabilidades para usuários;
III- especificar procedimentos mínimos para o controle de acesso lógico aos ativos de tecnologia da informação.

O controle de acesso lógico a ativos de tecnologia da informação no âmbito da PMRO busca atender aos seguintes princípios:
I- privacidade: respeito à privacidade dos usuários e a finalidade de tratamento dos dados pessoais;
II- confidencialidade: garante que somente o usuário autorizado possa acessar o ativo de informação;
III- segurança: previne os riscos de acessos indesejáveis e vazamento de informações tratadas pela PMRO;
IV- autenticidade: garante que usuários anônimos acessem somente os ativos de tecnologia da informação considerados públicos;
V- interoperabilidade e otimização de recursos: uso de tecnologias ou processos que atendam o maior número de ativos de tecnologia da informação, quando for viável;
VI- não repúdio: acurácia e precisão na identificação das atividades do usuário.

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Prefeitura Municipal de Rio das Ostras e/ou terceiros.
O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).
Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.
Todos os dispositivos de identificação utilizados na PMRO, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.
O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).
Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.
É proibido o compartilhamento de login para funções de administração de sistemas.
É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for afastado, o Departamento/Divisão onde o mesmo trabalhava deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. O mesmo procedimento deve ser feito pelo usuário afastado, uma vez que o

usuário e senha, são de total responsabilidade dele. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.
Caso o colaborador esqueça sua senha, ele deverá efetuar o procedimento para recuperação de senha pelo site: http://jubarte.riodasostras.rj.gov.br :

1.2. Tratamentos de incidentes

O processo de tratamento de incidentes de segurança deve considerar eventual violação deste normativo de controle de acesso lógico.
A permissão de acesso lógico que não implementar padrão de controle a partir de um dispositivo criptográfico, biometria ou senha deve ser tratada como incidente de segurança.
Pedido de análise de operação de um comportamento de usuário deve ser registrado pela área de negócio responsável pelo serviço ou por um grupo de trabalho que foi formalmente designado para investigar um incidente envolvendo o respectivo usuário.

1.3. Das responsabilidades dos envovidos

A Coordenadoria de Tecnologia da Informação (COTINF) é a unidade responsável por assegurar a execução das normas do controle de acesso lógico aos ativos de tecnologia da informação.
A área de negócio deve definir o direito de acesso lógico dos usuários ao respectivo serviço de tecnologia da informação por ela gerenciado.
O acesso lógico é atribuído a um usuário em observância às regras de negócios especificadas pelo operador do processo de negócio.
Todo direito de acesso lógico está condicionado à aprovação, ou validação, da respectiva pessoa responsável pelo processo de negócio, tais como: chefia de unidade organizacional, operador de dados ou coordenador de projeto registrado na instituição.
Todo serviço de tecnologia da informação mantido pela PMRO, adquirido ou desenvolvido a partir da publicação deste normativo, deve priorizar o uso de controle de acesso lógico com o uso da base de dados centralizada para autenticação institucional, bem como definir as responsabilidades para execução do controle de acesso lógico e gestão de usuário.

1.4. Computadores e recursos tecnológicos

Os equipamentos disponíveis aos usuários são de propriedade da PMRO, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.
É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, instalações de links de internet sem o conhecimento prévio e o acompanhamento de um técnico da COTINF, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à COTINF, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.
Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.
Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no atendimento.
A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.
Arquivos pessoais e/ou não pertinentes às atividades da PMRO (fotos, músicas, vídeos, etc..), não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente com ou sem comunicação prévia ao usuário.
Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.
É proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
Deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
Todos os recursos tecnológicos adquiridos pela PMRO devem ter imediatamente suas senhas padrões (default) alteradas.
Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.
Algumas situações em que é proibido o uso de computadores e recursos tecnológicos da PMRO.
tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
burlar quaisquer sistemas de segurança.
acessar informações confidenciais sem explícita autorização do proprietário, salvo em caso de imputação de crimes ou lesão a terceiros.
vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

1.5. Solicitação de acesso

O usuário deverá fazer uma solicitação da criação da conta, através do formulário eletrônico, disponível no site da Prefeitura através do link https://jubarte.riodasostras.rj.gov.br/pages/cartaSenha.
Neste formulário, deverá ser informado os dados do usuário, bem como os acessos que serão necessários para que este usuário desempenhe suas funções na área (diretórios da rede PMRO, acesso ao sistema de aplicação SALI, SIGA, Jubarte e outros, acesso ao e-mail e Internet).
Após o preenchimento do formulário, o mesmo deverá ser impresso e autorizado pela chefia imediata ou secretário da pasta, devidamente assinado por extenso (carimbo e matrícula) e anexado no sistema;
A equipe de TI fará a avaliação dos dados informados no formulário, tudo estando corretamente preenchido, os dados serão validados e a carta senha contendo o login e a senha serão encaminhados para o e-mail informado. Normas inerentes a Política de utilização da redes

disponíveis em: http://bit.riodasostras.rj.gov.br

2. POLÍTICA DE UTILIZAÇÃO DE E-MAIL

O objetivo desta norma é informar aos colaboradores da PMRO quais são as atividades permitidas e proibidas quanto ao uso do e-mail corporativo.
O uso do e-mail da PMRO é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a PMRO e também não cause impacto no tráfego da rede.
O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens;
O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-los. Se for solicitada a interrupção do envio, esta deve ser acatada e o envio não deverá mais acontecer;
É proibido o envio de grande quantidade de mensagens de e-mail (spam) que, de acordo com a capacidade técnica da rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política;
Situações em que é proibido aos colaboradores o uso do e-mail corporativo:
Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a PMRO vulnerável a ações civis ou criminais;
Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
É obrigatória a utilização de assinatura nos e-mails, seguindo padrão estabelecido pela PMRO (Anexo com o padrão).
Normas inerentes a Política de utilização de e-mail disponíveis em: http://bit.riodasostras.rj.gov.br

3. POLÍTICA DE ACESSO A INTERNET

Todas as regras atuais da PMRO visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a COTINF - ASCOMTI, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.
Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A COTINF - ASCOMTI, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.
A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas Secretarias.
É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.
O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.
Os usuários não poderão em hipótese alguma utilizar os recursos da PMRO para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.
Normas inerentes a Política de utilização de e-mail disponíveis em: http://bit.riodasostras.rj.gov.br

4. BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.
Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.
As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.
As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restaurações decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.
Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 90 ou 120 dias, de acordo com a criticidade do backup.
Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas,

o qual deverá ser preenchido pelos responsáveis e auditado pela equipe de Segurança da Informação.
Arquivo morto digital refere-se aos documentos que não são mais necessários para o dia-a-dia de uma empresa, mas que ainda precisam ser armazenados por um determinado período de tempo.
Toda virada de ano, os arquivos serão movidos para a pasta chamada “morto” e a nova estrutura do ano corrente será criada em espelho ao ano anterior, porém sem arquivos.
Os documentos do chamado arquivo morto servirão apenas para caráter de consulta a fim de manter a integridade do serviço realizado naquele período.
Normas inerentes a Política de Backup disponíveis em: http://bit.riodasostras.rj.gov.br

5. DATACENTER

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: fechadura eletrônica, biometria, cartão magnético entre outros.
O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.
O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.
Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.
A temperatura umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações, devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.
No caso de perda de chaves de departamentos ou laboratórios a coordenação responsável deve ser informada imediatamente para que possa providenciar a troca das fechaduras.
Normas inerentes a Política de DataCenter disponíveis em: http://bit.riodasostras.rj.gov.br

6. AUDITORIA

Todos os ativos de informação, de hardware, de software e intangíveis no âmbito da PMRO são passíveis de auditoria técnica a cargo da COTINF, segundo plano a ser estabelecido em norma específica.
Cabe a COTINF propor o plano de Auditoria e Conformidade que deverá incluir métodos, técnicas, procedimentos, normas e responsabilidades para o efetivo cumprimento do estabelecido por esta PSI no âmbito da PMRO.

7. DO TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

A PMRO manterá permanentemente uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) com a responsabilidade de receber, analisar e responder aos incidentes de segurança envolvendo computadores conectados à rede institucional de dados da PMRO.
Disponível no endereço: http://bit.riodasostras.rj.gov.brhttp://bit.riodasostras.rj.gov.br

8. DA GESTÃO DE RISCO

Um Plano de Gestão de Riscos deve ser elaborado e mantido pela PMRO, com base na legislação vigente, contendo necessariamente uma lista das ameaças mais prováveis e suas ocorrências, uma classificação dos riscos e alternativas para mitigá-los.
Disponível no endereço http://bit.riodasostras.rj.gov.br

9. DA GESTÃO DE CONTINUIDADE

http://bit.riodasostras.rj.gov.br

Faz-se necessária a adoção de um conjunto de procedimentos emergenciais, através da definição de um Sistema de Gestão de Continuidade de Negócios (SGCN), para a eventualidade da ocorrência de algum incidente de segurança da informação que possa causar interrupção na continuidade de processos organizacionais para a PMRO, decorrentes de desastres ou falhas em Ativos de Informação.
Disponível no endereço http://bit.riodasostras.rj.gov.br

9.1. TERMO DE COMPROMISSO

O termo de compromisso é utilizado para que usuários se comprometam formalmente em seguir a política de segurança, tomando ciência das punições impostas ao seu não cumprimento.
No termo de compromisso são reforçados os principais pontos da política de segurança e, deve ser assinado por todos os funcionários e demais colaboradores da PMRO. Sua renovação deve ser feita sempre que necessário.
Disponível em: http://bit.riodasostras.rj.gov.br

9.2. VERIFICAÇÃO DA UTILIZAÇÃO DA POLÍTICA

Para garantir que as regras mencionadas acima estão sendo cumpridas, a COTINF - ASCOMTI se reserva no direito de:

Implantar softwares e sistemas que monitoram e gravam todos os usos de Internet através da rede e das estações de trabalho da empresa;
Inspecionar qualquer arquivo armazenado na rede, estejam eles no disco local da estação ou nas áreas privadas da rede;

9.3 VIOLAÇÃO DA POLÍTICA, ADVERTÊN CIA E PUNIÇÕES

Ao detectar uma violação da política, a primeira coisa a fazer é determinar a sua razão, ou seja, verificar se a violação ocorreu por negligência, acidente, erro ou por desconhecimento da política vigente.
Nos termos da Política de Segurança, a COTINF - ASCOMTI procederá ao bloqueio do acesso ou ao cancelamento do usuário, caso seja detectado uso indevido com o intuito de prejudicar o andamento do trabalho ou pôr em risco a imagem da instituição.

É recomendado o treinamento dos usuários em segurança da informação, por meio de cartilhas, com o intuito de divulgar e conscientizar os funcionários e demais colaboradores sobre a política de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos usuários. Os treinamentos de reciclagem devem ser previstos quando necessários.
Caso seja necessário advertir o usuário pelo não cumprimento das normas estabelecidas neste documento, devem ser informados o superior imediato e o departamento de Recursos Humanos para interagir e manterem-se informados da situação.

Conforme previsto no Regime Jurídico Único, Lei 079/1994, o funcionário/colaborador poderá ser aplicada a penalidade no caso da irregularidade comprovada.
De acordo com a infração cometida, as seguintes punições serão: comunicação de descumprimento, advertência ou suspensão e demissão por justa causa.
Comunicação de descumprimento: Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto ao Departamento de Recursos Humanos na respectiva pasta do funcionário.
Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.
Demissão por justa causa: Nas hipóteses previstas no estatuto do servidor municipal.

Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo a Comissão, no uso do poder diretivo e disciplinar que lhe é atribuído, aplicar a pena que entender devida quando tipificada a falta grave.

DECRETO Nº 3623/2023

O PREFEITO DO MUNICÍPIO DE RIO DAS OSTRAS, Estado do Rio de Janeiro, no uso de suas atribuições legais e nos termos da Lei Municipal nº 2816/2022.

DECRETA

Art. 1º Fica aberto Crédito Adicional Suplementar em favor do Município de Rio das Ostras nas dotações orçamentárias constantes do Anexo Único deste Decreto na importância de R$220.000,00 (duzentos e vinte mil reais).
Art. 2º O recurso para atender o artigo 1º deste Decreto, fundamenta-se nos termos do inciso III, § 1º do artigo 43 da Lei Federal nº 4.320/64, em conformidade com Anexo Único do presente Decreto.
Art. 3º Este Decreto entra em vigor na data de sua publicação.

Gabinete do Prefeito, 07 de junho de 2023.

MARCELINO CARLOS DIAS BORBA
Prefeito do Município de Rio das Ostras

ANEXO ÚNICO DO DECRETO Nº 3623/2023

02 - MUNICÍPIO DE RIO DAS OSTRAS

UNIDADE ORÇAMENTÁRIA - PROGRAMA DE TRABALHO	CR	DESPESA - FONTE	ANULAÇÃO	REFORÇO
02.12 - 23.122.0001.2.151 SEDTUR - Manutenção da Unidade	0355	4.4.90.52.00 - 1.704.0104	20.000,00	
02.12 - 23.695.0035.2.505 SEDTUR - Fomento ao Turismo	0357	3.3.90.39.00 - 1.704.0104		20.000,00
02.16 - 27.811.0089.2.534 SEMEDE - Promoção e Participação em Eventos Esportivos e de Lazer	1741	3.3.90.32.00 - 2.704.0104		200.000,00
02.16 - 27.812.0089.2.537 SEMEDE - Manutenção de Unidades e Núcleos Esportivos	1751	4.4.90.52.00 - 2.704.0104	200.000,00	

TOTAL	220.000,00	220.000,00

DECRETO Nº 3624/2023

O PREFEITO DO MUNICÍPIO DE RIO DAS OSTRAS, Estado do Rio de Janeiro, no uso de suas atribuições legais e nos termos da Lei Municipal nº 2816/2022.

DECRETA

Art. 1º Fica aberto Crédito Adicional Suplementar em favor da Fundação Rio das Ostras de Cultura na dotação orçamentária constante do Anexo Único deste Decreto na importância de R$ 45.510,00 (quarenta e cinco mil, quinhentos e dez reais).
Art. 2º O recurso para atender o artigo 1º deste Decreto, fundamenta-se nos termos do inciso III, § 1º do artigo 43 da Lei Federal nº 4.320/64, em conformidade com anexo único do presente Decreto.
Art. 3º Este Decreto entra em vigor na data de sua publicação.

Gabinete do Prefeito, 07 de junho de 2023.