Anexo

- Anexo

Anexo

CHECKLIST NÍVEL 0

ITEM	OK?
As contas padrão de usuário não são contas de administrador, nem de administrador local ou equivalente.	
As contas de administrador dos servidores ou dos computadores que atuam como tal são geridas apenas pela equipe de Tecnologia de Informação e Comunicação do Órgão Setorial.	
Restringir as contas privilegiadas de usuário, tais como as contas de administrador, root e equivalentes, para que apenas os usuários que necessitam tais contas por necessidade de serviço, ou usuários que sejam servidores de carreira ou especialização em tecnologia da informação, possam ter permissão de uso de tais contas.	
As contas de acesso para os ativos de infraestrutura e de rede são geridas apenas pela equipe de Tecnologia de Informação e Comunicação do Órgão Setorial, pelo Integrador Estratégico ou pelo prestador de serviços de infraestrutura.	
Todas as senhas padrão dos ativos de infraestrutura e de rede que estiverem sob a gestão da equipe de Tecnologia de Informação e Comunicação do Órgão Setorial estão alteradas para uma senha não padrão, preferencialmente com o uso de caracteres e números no mínimo	
Todas as senhas padrão dos ativos de infraestrutura e de rede que estiverem sob a gestão da equipe de Tecnologia de Informação e Comunicação do Órgão Setorial são alteradas periodicamente, pelo menos a cada três anos ou sempre que for necessário, para uma outra senha não padrão, preferencialmente com o uso de caracteres e números não utilizados na senha anterior.	
Existe um aceite formal dos servidores, admitido o uso de meio eletrônico/digital, explicitando o conhecimento e a concordância com as Políticas de Segurança implantadas no Órgão Setorial	

É executada uma varredura periódica, no mínimo anualmente, para identificar os usuários que não são mais utilizados (ex: usuários dos servidores que já foram exonerados).	
É executado um procedimento periódico, no mínimo anualmente, para bloquear e/ou eliminar os usuários inativos, isto é, os usuários que não são mais exonerados.	
Existe um documento corporativo (ou equivalente) atualizado periodicamente com os sistemas utilizados no Órgão Setorial e os respectivos procedimentos para solicitação de acesso.	
O documento corporativo (ou equivalente) atualizado com os sistemas está armazenado em um repositório corporativo, e não pessoal, do Órgão Setorial.	
Existe um procedimento corporativo para concessão de permissões de acesso a usuários, registrando-se os pedidos de concessão, preferencialmente por meio eletrônico.	
Existe um procedimento corporativo que define formalmente quem é o autorizador da concessão de permissão de acesso, sendo que o autorizador não pode ser o próprio usuário, salvo no caso do Secretário, Secretário Adjunto, Subprefeito, Chefe de Gabinete e equivalentes.	
Existe um procedimento corporativo que define formalmente os critérios de exclusão de permissão de acesso, incluindo no mínimo os casos de bloqueio/exclusão do usuário e a remoção em caráter fático do servidor.	
É executada uma varredura e adequação periódicas das permissões concedidas a cada usuário, excluindo-se as permissões que não sejam estritamente necessárias ao cumprimento das atividades atuais do usuário.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que são adotados critérios e procedimentos para se ter senhas adequadamente fortes para os usuários e ativos do Órgão Setorial que são geridos pelas entidades supra.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que são adotados políticas de aplicação de patches do sistema operacional e de outras aplicações, para eliminar vulnerabilidades conhecidas.	

Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que existem medidas para a proteção dos endpoints do Órgão Setorial geridos pelos mesmos, seja por meio de uma solução integrada ou por meio de um conjunto de soluções, incluindo pelo menos um antivírus.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que existem medidas para a proteção da rede wireless do Órgão Setorial gerida pelos mesmos, configurando no mínimo o protocolo WPA2 para segurança.	
Existe um sistema de gestão de ativos implantado, operacional e em utilização no Órgão Setorial para gerir os ativos de microinformática (essencialmente desktops, notebooks e similares).	
Existe um procedimento corporativo, de preferência formal, que permite à equipe de Tecnologia de Informação e Comunicação do Órgão Setorial localizar e copiar para o repositório corporativo, de ofício, os dados corporativos armazenados em equipamentos pessoais, especialmente para o caso de remoção, aposentadoria e/ou exoneração iminente do servidor.	
Existe um procedimento corporativo implantado, junto com a infraestrutura necessária, para a execução de rotinas básicas de backup de dados, considerando a Orientação Técnica sobre o tema.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que existem medidas para limitar o acesso direto à base de dados do Órgão Setorial, de forma que o acesso seja realizado estritamente em função das necessidades de serviço.	