GERED/COSEI

CÓDIGO	TÍTULO	VIGÊNCIA	VERSÃO
NORMA 004/2020	NORMA DE USO DE DISPOSITIVOS MÓVEIS PARTICULARES (BYOD)	28/12/2020	1

1 PREFÁCIO

A presente Norma está de acordo às diretrizes da Política de Segurança da Informação e Comunicação do CIASC.

2 OBJETIVO

Normatizar a abrangência, os processos e responsabilidades inerentes ao uso de Dispositivos Móveis BYOD (*Bring Your Own Device*, ou traga seu próprio dispositivo), visando à permissão de uso destes dispositivos para fins profissionais, no âmbito do CIASC.

3 ESCOPO

Esta Norma se aplica a todos os usuários (clientes, prestadores de serviços, estagiários, empregados, visitantes...) que utilizam os recursos computacionais do CIASC para acesso à internet e rede local (LAN), cabeada e sem fio.

4 TERMOS E DEFINIÇÕES

Para efeito desta Norma aplicam-se os seguintes conceitos e definições:

Segurança da Informação e Comunicação (SIC) – proteção da informação contra ameaças para garantir a continuidade das atividades finalísticas e meio da instituição, minimizar os riscos e maximizar a eficiência e a efetividade das ações realizadas no CIASC.

Incidente em Segurança da Informação – qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações da instituição ou ameaçar a segurança da informação.

Usuário – qualquer pessoa (clientes, prestadores de serviços, estagiários, empregados, visitantes...) que possua ou não ligação com a empresa, e que necessite de acesso a um sistema ou recurso computacional do CIASC.

Usuário institucional – Usuário que, consideradas as atividades finalísticas e administrativas do CIASC, necessita acesso a Serviços de TIC institucionais e que possui vínculo formal vigente com o CIASC, temporário ou permanente (empregados, estagiários, empregados temporários ou terceirizados).

Usuário externo – Usuário que não contempla os requisitos de "Usuário institucional" e que, consideradas as atividades finalísticas e administrativas do CIASC, necessita acesso a Serviços de TIC institucionais de forma temporária (participantes de eventos, colaboradores ou prestadores de serviço cuja forma de relação temporária com a instituição preveja a necessidade de acesso por tempo limitado a um ou mais Serviços de TIC institucionais).

Serviços de TIC institucionais – Serviços de TIC providos na unidade do CIASC por meio de recursos próprios ou contratados pela instituição para a viabilização das suas atividades finalísticas (Desenvolvimento, Pesquisa e Suporte) e administrativas, planejados e operacionalizados pelas equipes responsáveis.

Serviço de conectividade – Serviço de TIC que inclui os recursos computacionais de interconexão a rede local das unidades, por meio de acesso aos ativos de rede cabeada ou sem fio, planejados e implantados para viabilizar o acesso aos Serviços de TIC institucionais e aos serviços não institucionais disponíveis pela Internet que estejam alinhados com as atividades finalísticas (Desenvolvimento, Pesquisa e Suporte) e administrativas do CIASC, a partir de equipamento computacional institucional ou de propriedade pessoal do usuário.

Serviço de impressão e digitalização – Serviço de TIC que inclui os recursos computacionais necessários à impressão e digitalização de documentos que estejam alinhados com as atividades finalísticas (Desenvolvimento, Pesquisa e Suporte) e administrativas do CIASC.

Dispositivo BYOD (*Bring Your Own Device*) – é qualquer equipamento de propriedade pessoal do usuário, isto é, que não esteja tombado na instituição, como parte do seu patrimônio ou depositado nesta em função da execução de projetos de desenvolvimento, pesquisa ou suporte, que seja eventual ou frequentemente usado no âmbito do CIASC para acesso a Serviços de TIC Institucionais, bem como transportado e utilizado em ambiente externo aos limites físicos da instituição, por meio de conexão com redes de acesso institucionais. São exemplos de Dispositivos Móveis: *smartphone*, *ultrabook*, *notebook* e *laptop*.

Redes de acesso local corporativa – conjunto de redes físicas e lógicas utilizadas para acesso de dispositivos à rede de dados, classificadas em duas dimensões: Sem fio e Cabeada. A organização das redes lógicas (VLANs) deve respeitar os padrões de equalização especificados pela Coordenadoria de Gestão de Redes (CORED).

VLAN – Uma Rede Local Virtual, normalmente denominada de VLAN (*Virtual Local Area Network*), é uma rede logicamente independente. Várias VLANs podem coexistir em um mesmo comutador (*switch*), de forma a dividir uma rede local (física) em mais de uma rede (virtual), criando domínios separados.

MAC *Address* – Um endereço de Controle de Acesso à Mídia (endereço MAC) de um dispositivo é um identificador único atribuído a uma interface de rede (ou *Network Interface Controller* - NIC).

5 PAPEIS E RESPONSABILIDADES

5.1 Usuário

- Manter sigilo das informações de acesso ao ambiente de rede do CIASC, sendo de sua total e exclusiva responsabilidade qualquer operação realizada por meio de suas credenciais de acesso à rede local;

- Fazer o uso consciente dos recursos computacionais do dispositivo em ambiente corporativo e da rede de dados;
- Comunicar imediatamente à área de Segurança da Informação (COSEI) qualquer situação que coloque em risco o acesso ao ambiente da rede de dados do CIASC;
- Informar seu gestor quando forem identificados direitos de acesso à rede desnecessários à execução de suas atividades; e
- Manter o Sistema Operacional do dispositivo BYOD atualizado e com ferramentas de segurança (*firewall*, antivírus, etc.) ativas e atualizadas;

5.2 Gestor

- Conscientizar os usuários em seu domínio administrativo quanto às orientações presentes neste documento e nas boas práticas de segurança; e
- Comunicar imediatamente à área de Segurança da Informação (COSEI) caso verifique qualquer ameaça, vulnerabilidade ou situação que possa colocar em risco o ambiente computacional e a rede em questão.

5.3 Gerência de *Data Center* (GEDAT)

- Manter os registros dos sistemas de autenticação do CIASC para fins de auditoria, respeitando a legislação e as boas práticas de mercado;
- Manter registro histórico de solicitações de criação e revogação de usuários para fins de auditoria e controle; e
- Efetuar auditorias no ambiente como forma de garantir que os mecanismos de segurança adotados se mantêm eficientes.

5.4 Gerência de Redes (GERED)

- Administrar a segregação de acesso lógico, através de VLANs, entre os ambientes de acesso a visitantes e à rede local do CIASC;

- Administrar os acessos lógicos do ambiente de rede de dados do CIASC, em *firewall* apropriado para este acesso;
- Manter a disponibilidade, integridade e confidencialidade em todo o ambiente lógico;
- Monitorar todo o ambiente de modo a identificar proativamente anomalias e acessos maliciosos;
- Manter os registros de acesso para fins de auditoria, respeitando a legislação e as boas práticas de mercado;
- Manter registro histórico de solicitações de criação e revogação de usuários visitantes na rede SisCAV (Sistema de Controle e Autenticação de Visitantes) para fins de auditoria e controle; e
- Efetuar auditorias no ambiente como forma de garantir que os mecanismos de segurança adotados se mantêm eficientes.

5.5 Gerência de Recursos Humanos (GEREH)

- Notificar à equipe da GEDAT/COAPE (Coordenadoria de Ambiente Operacional) a criação ou revogação de credenciais de acesso remoto de funcionários admitidos ou demitidos; e
- Conscientizar os novos funcionários quanto às orientações presentes neste documento e nas boas práticas de segurança.

6 DIRETRIZES

6.1 Os funcionários do CIASC poderão fazer acesso à rede do local cabeada do CIASC e à rede sem fio “AP-CIASC”, utilizando seu dispositivo BYOD, desde que possuam uma credencial própria e válida nos sistemas de autenticação do CIASC para o acesso.

6.2 Caso o funcionário opte apenas pelo acesso à Internet de seu BYOD, sem o acesso aos demais serviços de rede local corporativa, como VoIP, Impressão, etc.., deverá utilizar a rede sem fio “AP-VISITANTE” e autenticar-se através de um cadastro

automático de seu dispositivo no sistema SisCAV. Esta forma não exime o funcionário de qualquer responsabilidade contida nesta Norma.

6.3 Os usuários externos, terceirizados e prestadores de serviços poderão utilizar os dispositivos BYOD através da rede sem fio “AP-VISITANTE”, autenticando-se através de um cadastro automático de seu dispositivo no sistema SisCAV. O acesso a recursos corporativos locais não será permitido. Esta forma não exime o usuário de qualquer responsabilidade contida nesta Norma.

6.4 O acesso corporativo via rede cabeada é proibido para acesso de prestadores de serviços, terceirizados e visitantes. Apenas poderá ser acessado mediante autorização formal da área de Segurança da Informação (COSEI) e deverá ser acompanhado pelo funcionário do CIASC responsável pela demanda.

6.5 A COSEI poderá, sem aviso prévio, suspender o acesso em caso de suspeita de incidentes de segurança da informação. Nesses casos, o dispositivo estará sujeito à coleta de informações de *hardware* e *software* exclusivamente por meio da coleta de tráfego da rede interna ou externa, ressalvada a privacidade do usuário. Em casos de comprovação de incidentes de segurança da informação, que envolva os dispositivos móveis BYOD, o acesso será revogado e serão realizadas as devidas providências administrativas para apuração da responsabilidade.

6.6 Os *softwares* utilizados nos dispositivos BYOD deverão possuir licenças para não haver implicações legais em se tratando de pirataria de *software*, sendo o usuário o único responsável pela manutenção e atualização das licenças dos *softwares* instalados no seu dispositivo. O proprietário responderá por qualquer incidente ou processo sobre o uso de *software* não licenciado em seu dispositivo.

6.7 É responsabilidade do proprietário, a guarda e manutenção adequada do dispositivo BYOD. O CIASC não se responsabiliza por acessos indevidos no dispositivo ou danos de *hardware* e/ou *software* que possam ocorrer neste quando usado no contexto da instituição. A responsabilidade de proteção física e lógica do dispositivo BYOD é exclusiva do proprietário.

6.8 Os usuários: empregados, terceirizados ou prestadores de serviço não poderão armazenar informações críticas, confidenciais em seus dispositivos BYOD, como

documentos e *backups* do CIASC que possam comprometer a segurança destas informações em caso de roubo ou extravio dos mesmos.

6.9 Em caso de perda, roubo ou furto do dispositivo utilizado, deverá ser informado imediatamente à COSEI, via Sistema de Chamados GLPI, para serem tomadas as medidas cabíveis de segurança e, assim, evitar o uso indevido por terceiros, dentro do ambiente do CIASC ou VPN, do dispositivo extraviado.

6.10 É responsabilidade exclusiva do proprietário do dispositivo a segurança dos dados no mesmo para não haver o vazamento de informações ou perda de dados. Recomenda-se a utilização de criptografia nos dados do dispositivo e *backup* frequente dos dados pessoais, bem como o uso de *software* de *firewall* e antivírus.

6.11 Qualquer utilização de dispositivos BYOD estará sujeita às regras previstas na Política de Segurança de Informação do CIASC.

6.12 A COSEI poderá solicitar a instalação de *softwares* adicionais para controle dos dispositivos BYOD para garantir a conformidade dos controles de segurança para acesso à rede.

7 SANÇÕES

A violação desta política por qualquer usuário será reportada ao CGSI - Comitê Gestor de Segurança da Informação do CIASC e ao superior imediato que liberou o acesso e que poderá tomar medidas para suspender de forma imediata, temporária ou permanente os seus privilégios de acesso à rede local de dados, bem como encaminhar os fatos às áreas pertinentes para aplicação das medidas administrativas cabíveis com vistas a impor as sanções aplicáveis, seja no âmbito de responsabilização interna, através de sanções disciplinares, seja no âmbito externo, às pessoas físicas ou jurídicas, tais como multas e demais sanções previstas em contratos, respeitado o princípio da proporcionalidade e do devido processo legal, sem prejuízo de eventual ação judicial para reparação dos danos e preservação dos direitos desta empresa.

8 REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação - Técnicas de segurança - Código de prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2013.

9 HISTÓRICO DE VERSÕES

Alterações	Data de aprovação	Versão gerada