Autor: Oi – Segurança de Informações
Última Revisão: 24/05/2013.
Versão: 5
Classificação: **CONFIDENCIAL**

Requisitos para conectividade de parceiros e fornecedores

Atenção

* O termo PARCEIRO ou PARCEIROS empregado neste documento refere-se tanto a parceiros, fornecedores ou quaisquer outras entidades que não sejam parte da própria Oi.

APRESENTAÇÃO

Este documento apresenta os requisitos mínimos a serem adotados pelos PARCEIROS* que desejarem acesso ao ambiente corporativo da Oi através de links, VPNs ou similares.

REQUISITOS

Para que seja autorizado o acesso ao ambiente corporativo da Oi através do ambiente de PARCEIROS, estes devem:

1) Elaborar projeto de conectividade e viabilidade técnica junto a Gerencia de Suporte a Software e Rede da Oi;
    a. A tecnologia a ser empregada deverá garantir que as informações trafeguem em meio seguro;
    b. O projeto deverá receber aceite formal da área de Segurança da Informação da Oi.
2) Fornecer à Oi informações completas de contato da equipe que deverá ser acionada em caso de incidentes ou necessidade de verificações:
    a. NOME COMPLETO;
    b. CPF;
    c. TELEFONE MÓVEL (OI preferencialmente);
    d. TELEFONE FIXO;
    e. E-MAIL ou Lista de Distribuição.
3) Fornecer à Oi listagem completa de ativos e/ou aplicações da Oi a que necessitará conectividade, incluindo-se Perfis, IPs e Portas;
4) Declarar que o PARCEIRO:
    a. Tem ciência de que é proibida a utilização de qualquer outro meio de acesso à Oi, incluindo acesso em ambiente interno ou via VPN Oi.
    b. Manterá a Oi sempre atualizada quanto às alterações dos itens 2 e 3 deste documento;
    c. Autoriza que a Oi utilize internamente e informe os dados do PARCEIRO e/ou de seus prestadores às autoridades legais sempre que necessário;
    d. Sob nenhuma hipótese permitirá o compartilhamento de credencias/senhas no ambiente do PARCEIRO e nem entre pessoas vinculadas a si, e que todos os seus funcionários e/ou prestadores de serviço possuirão credenciais individuais e os privilégios necessários antes de ter acesso à quaisquer ativo ou informação da Oi;
    e. Sob nenhuma hipótese realizará automações ou alterações em ativos Oi sem autorização expressa da mesma;
    f. Sob nenhuma hipótese utilizará em seu ambiente softwares, mídias ou ativos não licenciados;
    g. Sob nenhuma hipótese explorará vulnerabilidades eventualmente existentes em sistemas, ativos ou processos da Oi e informará imediatamente à Oi, através de abertura de chamado para o agente de solução CSIRT via Help Desk Oi (0800.282.0031), toda e qualquer vulnerabilidade de que tiver conhecimento ou venha a conhecer;

* O termo PARCEIRO ou PARCEIROS empregado neste documento refere-se tanto a parceiros, fornecedores ou quaisquer outras entidades que não sejam parte da própria Oi.

h. Entende que a conectividade entre o ambiente corporativo da Oi e o ambiente do PARCEIRO é um benefício provisório que poderá, a qualquer momento, ser bloqueada, alterada, cancelada ou interrompida sem aviso prévio;
i. Possui mecanismos de contingencia para conectividade à Oi caso o mecanismo padrão torne-se indisponível, garantindo que os serviços prestados não sejam afetados;
j. Caso a Oi opte por substituir a qualquer tempo o mecanismo de conectividade por qualquer outra tecnologia ou ainda caso a Oi decida agregar ao modelo atual de conectividade qualquer tipo de requisito adicional (físico ou lógico), o PARCEIRO reconhece como legítimo e assume o compromisso por arcar, sem qualquer ônus para a Oi, com os custos referentes (licenciamentos, *tokens*, *simcards*, custos telefônicos, etc.);
k. Utiliza mecanismos de autenticação, compatíveis com os sistemas internos da Oi, a fim de que se conectem a estes, exclusivamente para os casos de prestação de serviços remotos. Para a ativação dos mecanismos de autenticação, são necessários *chips*, os quais deverão ser requeridos à OI, às expensas do PARCEIRO;
l. Arcará com o custo necessários (incluindo licenciamento e infraestrutura) caso seja necessária utilização de recursos Oi;
m. É responsável por toda ação executada no ambiente Oi ou através do mesmo, assumindo o compromisso de restituir (ou indenizar) à Oi, imediatamente, qualquer prejuízo eventual;
n. Isenta a Oi de qualquer responsabilidade quanto às ações realizadas por intermédio da conectividade;
o. Compromete-se a não fazer nenhum uso (incluindo, mas não se limitando a Visualização, Armazenamento, Divulgação, Compartilhamento e Comercialização), além daquele estritamente necessário ao cumprimento de suas obrigações com a Oi, dos ativos, aplicações, processos, serviços, dados ou informações a que tiver acesso;
p. Implementa controles que garantem a destruição das mídias de armazenamento não mais em uso;
q. Destruirá toda informação que esteja em sua posse no término de seu contrato com a Oi;
r. Aceita e reconhece como legítimas todas as normas legais brasileiras e as normas e regulamentos internos da Oi (atuais e futuras);
s. A conectividade com a Oi somente estará acessível via ambiente que:
    i. Seja totalmente segregado (física e logicamente);
    ii. Possua total controle de acesso, havendo controle e registro de cada pessoa e ativo tecnológico que acesse ou deixe o local;
    iii. Possua equipe de segurança física 24x7x365;
    iv. Possua câmeras de vigilância e monitoração 24x7x365, inclusive contra incêndio;
    v. Possua inventário de todos os ativos tecnológicos do ambiente:
        1. Tipo;
        2. Fabricante;

* O termo PARCEIRO ou PARCEIROS empregado neste documento refere-se tanto a parceiros, fornecedores ou quaisquer outras entidades que não sejam parte da própria Oi.

3. Número de série;
4. IP, SO e MAC quando aplicável;

vi. Garanta:

1. não haver risco de que outras redes da empresa tenham comunicação com este ambiente;
2. não haver risco de que este ambiente seja acessado por dispositivos móveis ou sem fio;
3. não haver risco de que haja fuga de informações através de pendrives, máquinas fotográficas, papéis, lixeiras ou quaisquer outros meios;
4. não haver risco de que este ambiente seja acessado remotamente ou através da Internet. Nota: Se for essencial que funcionários do parceiro possuam acesso remoto (VPN) ao ambiente para a execução de suas atividades, o parceiro deverá adotar:
    a. Criptografia segura na comunicação;
    b. Identificação única para seus usuários;
    c. Bloqueio de acessos simultâneos;
    d. Autenticação baseada em validação de usuário+senha e dispositivos físicos, tais como: Tokens, SmartCards ou Validadores de Impressões Digitais.
    e. Restrição baseada em horário de utilização;
    f. Restrição baseada em local de utilização;
    g. Revisão de acesso periódica removendo direitos de usuários já desligados;
    h. Revisão de acesso periódica removendo direitos de usuários que não utilizaram o serviço nos últimos 45 dias;
    i. Guarda dos registros de autenticação, demonstrando o usuário, IP de origem, IP Interno, Data/Hora e Fuso, evento (sucesso e falha) por pelo menos 5 anos, independentemente da manutenção com o contrato com a Oi.

t. Adota controles que bloqueiam a execução de vírus e outros *malwares* em seu ambiente;

u. Aplica todas as atualizações e patches de segurança em seu ambiente num prazo máximo de 48 horas após a liberação pelo fabricante, exceto nos casos em que a atualização incompatibilize o ativo ou sistema com o ambiente Oi, nestes casos a Oi deverá ser informada formalmente da impossibilidade de realizar a atualização e da inexistência de soluções de contingencia;

v. Possui auditoria completa armazenada pelo período mínimo de 5 (cinco) anos sobre todos os eventos realizados em seu ambiente ou a partir do mesmo e os responsáveis;

w. Permite que a Oi ou quem ela indique possa auditar a qualquer tempo, sem necessidade de comunicação ou aviso prévio tudo o que foi declarado, inclusive, podendo,

mas não se limitando, realizar visitas nos ambientes internos do PARCEIRO, ter acesso a documentos e acessar seus dispositivos e ativos.

i. O PARCEIRO compromete-se a viabilizar todos os requisitos de acessos físicos e/ou lógicos necessários.

x. Tem ciência de que ao detectar ou ser avisada formalmente de qualquer conduta e/ou método considerado inadequado, ilegal, imoral, ofensivo ou antiético por parte do Parceiro, a OI poderá, a seu exclusivo critério, e independentemente de prévia notificação, proceder à imediata suspensão ou cancelamento dos serviços e benefícios oferecidos pela OI ao Parceiro, sem prejuízo de pleitear indenização por eventuais perdas e danos incorridos pela OI em decorrência da conduta do Parceiro.

y. Tem ciência de que as informações técnicas e operacionais, possuem caráter confidencial não podendo ser transmitidas ou facilitadas a quem quer que seja sem a expressa autorização da Oi, respondendo o Parceiro em função de sua divulgação, sem prejuízo das cominações legais.

z. Possui documentos que comprovem todas as declarações anteriores e possui conformidade (não é necessário apresentar certificação) com as normas ISO 27001, ISO 27002, Sarbanes Oxley e PCI;

* O termo PARCEIRO ou PARCEIROS empregado neste documento refere-se tanto a parceiros, fornecedores ou quaisquer outras entidades que não sejam parte da própria Oi.