Anexos do Acordo de Sede da COP 30

Anexo V: Segurança da informação e cibernética

1. Escopo / modalidade

1.1. Os Serviços de Cibersegurança da COP 30 serão coordenados sob a liderança do ponto focal de segurança do Secretariado e do ponto focal de segurança cibernética do Governo.

1.2. Os Serviços de segurança cibernética deverão estabelecer as seguintes medidas principais com vista à preparação e execução de um plano eficaz de preparação e Defesa e resposta em caso de incidente de segurança cibernética.

1.2.1. Apoiar a concepção e a implementação dos serviços de TIC.

1.2.2. Realizar o planejamento, análise, concepção e a implementação de medidas de proteção, monitoramento e resposta por especialistas em segurança cibernética e segurança da informação para os sistemas de reuniões/conferências pré-sessões, incluindo as infraestruturas TIC, conforme identificadas e detalhadas no plano do projeto TIC.

1.2.3. Realizar uma auditoria de segurança da concepção e implementação das TIC.

1.2.4. Preparar a resposta a Incidentes em caso de incidente de segurança cibernética, incluindo a preparação de uma resposta abrangente e coordenada à segurança cibernética em caso de riscos e/ou ataques persistentes à segurança cibernética.

1.3. O responsável pela segurança da informação do Secretariado é o ponto focal. O governo designará um representante para atuar como seu ponto focal de segurança cibernética e segurança da informação. Será elaborado um plano de segurança cibernética em consulta com o Secretariado, a incluir no plano global do projeto de TIC.

1.4. A segurança cibernética nas instalações da Conferência (conforme acordado no Acordo do País Anfitrião-HCA) será da responsabilidade do Secretariado e será realizada em estreita colaboração com as autoridades de segurança cibernética do Governo. Os termos da cooperação serão claramente definidos pelo Governo e pelo Secretariado no presente anexo. O Secretariado e o Governo cooperarão em matéria de inteligencia cibernética e na preparação de uma resposta abrangente de segurança cibernética em caso de ameaças persistentes e de ataques à segurança cibernética.

1.5. O Secretariado se compromete a trabalhar com o governo e o principal contratante de segurança cibernética que será contratado pelo Secretariado em conformidade com as regras e regulamentos da ONU para garantir o mais alto nível de informação e segurança cibernética. A seleção dos contratantes será feita numa base concorrencial e todas as propostas serão discutidas e acordadas com o Governo.

1.6. A segurança cibernética fora das instalações da Conferência permanecerá sob a responsabilidade do Governo.

2. Apoio à concepção e implementação de sistemas de tecnologia da informação

2.1. Os especialistas em segurança cibernética e da informação deverão participar e auxiliar na concepção e implementação seguras dos sistemas de tecnologia da informação estabelecidos para dar suporte a Conferência.

2.1.1. Participação nas reuniões de concepção Pré-Conferência.

2.1.2. Participação na fase de Prova De Conceito (POC) dos preparativos da Conferência (Ver resumo no apêndice abaixo).

3. Proteção/prevenção

3.1. Os especialistas em segurança cibernética e em segurança da informação devem realizar uma auditoria de segurança Pré-Conferência dos sistemas de informação a utilizar nas reuniões/conferências pré-sessões.

3.1.1 A auditoria deve avaliar a segurança dos sistemas informáticos e de rede, incluindo a infraestrutura, estações de trabalho individuais, sistemas/equipamentos habilitados para IP e aplicações críticas (por exemplo, Sistema de Registo).

3.1.2 O âmbito da auditoria deve incluir a segurança do software dos sistemas, bem como os controles físicos, tais como a proteção contra incêndios, a segurança física dos equipamentos TIC e a gestão da energia (ou seja, cabeamento, racks, sistemas de controle de acesso, impressoras, etc.).

3.1.3 Um relatório de auditoria pré-conferência deve ser apresentado o mais tardar duas semanas antes do início das reuniões/conferências pré-sessão.

3.1.4 Antes do início das reuniões/conferências pré-sessões, a equipe conjunta de segurança cibernética efetuará uma verificação pós-auditoria para verificar se as recomendações foram plenamente aplicadas. No final da conferência será apresentado um relatório de auditoria final ao Secretariado e ao Governo.

3.2. Os especialistas em segurança cibernética e segurança da informação devem:

3.2.1 Desenvolver uma avaliação das ameaças e dos riscos para as reuniões pré-sessões/Conferência em tempo hábil, de modo que o Secretariado e os diferentes fornecedores de TIC designados pelo Governo possam implementar ações de mitigação.

3.2.2 Apoiar o Secretariado e os diferentes fornecedores de TIC designados pelo Governo na resolução de quaisquer achados de auditoria pré-conferência.

3.2.3 Apoiar a implementação de configurações seguras para equipamentos TIC, incluindo, entre outros, pontos de acesso sem fios, impressoras, telefones celulares e sistemas/ equipamentos habilitados para IP, a fim de prevenir possíveis violações ou sequestros das conexões ou dispositivos.

3.2.4 Apoiar a implementação de uma comunicação segura na rede do local das reuniões pré-sessões/Conferências.

3.2.5 Avaliar a segurança dos sistemas de videovigilância dos centros de dados TIC.

3.2.6 Avaliar a frequência e a segurança do sistema de rádio utilizadas para apoiar as reuniões pré-sessões/Conferências.

3.2.7 Garantir que todos os computadores fornecidos pelo Governo em apoio às reuniões pré-sessões/Conferências estejam atualizados no que diz respeito aos patches de segurança e protegidos utilizando a solução Microsoft Defender for Endpoint.

3.3 O acesso a salas protegidas ou a outras estruturas físicas que abriguem e protejam equipamentos de TIC deve ser restrito ao pessoal autorizado (por exemplo, controle de chaves fisicas, listas de acesso eletrônico controladas).

3.4. No final da Conferência, o contratante de segurança cibernética deverá coordenar e assegurar a higienização de todos os equipamentos de TIC utilizados nas instalações da Conferência, de modo que as informações não possam ser recuperadas com esforço razoável. Sempre que aplicável, o Governo, por meio de seus representantes na área de TIC, deverá fornecer evidências de que a higienização foi realizada conforme exigido.

4. Monitorização/detecção

Anexos do Acordo de Sede da COP 30

4.1 Os especialistas em segurança cibernética e segurança da informação deverão:

4.1.1 Fornecer, configurar e monitorizar uma solução de Gestão de Informações e Eventos de Segurança (SIEM) que será utilizada para a coleta centralizada de registros (logs) dos sistemas, incluindo firewalls, equipamentos de rede, controladores de domínio, servidores de gestão de rede, firewalls de aplicações web.

4.1.2 Monitorizar a presença na Internet do site da Conferência, redes sociais e outros sites relacionados à Conferência.

4.1.3 Monitorar o ciberespaço em busca de ameaças e informações relacionadas à Conferência.

4.1.4 Monitorizar as redes sociais e a presença digital relacionada à COP 30 para garantir a integridade, incluindo as contas do Twitter da Secretária Executiva, da Presidência da COP e de outras autoridades VIPs e das páginas web oficiais da COP 30 (será fornecida uma lista de contas de redes sociais e páginas web essenciais aos especialistas em segurança da informação).

4.1.5 Projetar, construir e monitorar operações de segurança cibernética no Centro de Operações de Segurança (SOC) para realizar monitoramento contínuo em tempo real (24 horas por dia, 7 dias por semana) dos sistemas de TIC utilizados nas instalações da Conferência.

4.1.6 Prestar apoio presencial entre as 7h30 e as 22h durante as reuniões pré-sessões/Conferências, salvo indicação em contrário. O controle deve estar ativo fora do horário de expediente, com sistemas de alerta adequados. Caso o monitoramento após o expediente seja realizado remotamente, a comunicação entre os sistemas do local e o local de monitorização deverá obedecer ao mesmo nível de segurança como se estivesse sendo realizada no local.

5. Informações sobre ameaças

Um mês antes do início da Conferência, as informações sobre ameaças cibernéticas devem ser reunidas para determinar se quaisquer ameaças cibernéticas adicionais ou incomuns podem afetar a realização bem-sucedida da Conferência. O processo de informação sobre ameaças deverá prosseguir ao longo da conferência e duas semanas depois. Devem ser apresentados relatórios sobre qualquer informação identificada, incluindo o nível estimado de ameaça.

6. Resposta

Ao longo das reuniões pré-sessões/Conferências, uma equipe de resposta a emergências, composta por especialistas em segurança cibernética e segurança da informação e membros do Secretariado, deverá estar preparada para responder a ataques e ameaças de segurança cibernética ou de segurança da informação. Caso tal evento ocorra, a resposta adequada deverá ser realizada em estreita coordenação com o Secretariado.

6.1 Os especialistas em segurança cibernética e segurança da informação devem coordenar-se com o Secretariado para desenvolver e documentar um processo de gestão de incidentes antes do início das reuniões pré-sessões/Conferências. Esse processo deve incluir ações como identificação, categorização, comunicação e resposta em caso de qualquer ameaça ou ataque.

6.2 Com base na categorização da ameaça ou ataque e na localização do incidente, o coordenador de turno do Centro de Operações da Rede de TI (NOC) coordenará com o Secretariado para incidentes dentro das instalações da Conferência ou com o Governo para

incidentes fora das instalações da Conferência, a fim de recomendar um plano de ação em resposta ao incidente e dar continuidade a resposta até que o incidente seja mitigado.

6.3 Quando necessário, será fornecido suporte forense de segurança cibernética pelo fornecedor e pelo Governo, caso este disponha de capacidades adicionais. Em caso de ciberataque, o Secretariado, sem prejuízo dos privilégios e imunidades de que gozam o Secretariado e as Nações Unidas, solicitará, nos termos do quadro jurídico acordado do Acordo, a assistência do Governo para investigar o ocorrido, com vistas a instaurar medidas legais contra os autores do ataque. O Secretariado, no âmbito dos privilégios e imunidades que lhe são conferidos, e o governo cooperarão plenamente nesse sentido.

6.4 Os especialistas em segurança cibernética e segurança da informação devem apresentar um relatório escrito relativo a cada incidente de grande relevância, conforme definido no processo de gestão de incidentes.

7. Relatórios diários e reuniões

7.1 O Fornecedor de Segurança Cibernética deverá apresentar, todas as manhãs, um relatório diário sobre o status da segurança cibernética, referente ao dia anterior, contendo todas as questões identificadas relacionadas à segurança cibernética da Conferência

7.2 As Partes realizam reuniões diárias sobre o estado das operações de rede e das operações de segurança cibernética e da informação.

7.3 O Coordenador dos serviços de TIC do Secretariado prestará orientação e assistência para garantir a prestação segura dos serviços de TI durante as reuniões pré-sessões/Conferências.

8. Comunicação segura

O Governo deverá utilizar os serviços de colaboração em nuvem do Secretariado para garantir a comunicação segura e o compartilhamento de informações entre o Governo, os especialistas em segurança cibernética e segurança da informação e o Secretariado.

9. Responsabilidades específicas e competências

Os especialistas em segurança cibernética e em segurança da informação deverão possuir as seguintes áreas de responsabilidade e competências técnicas.

9.1 Áreas de responsabilidade: segurança dos terminais (endpoint), segurança das redes, segurança da Internet, auditoria de segurança física dos equipamentos informáticos, controle de acesso, segurança de páginas Web, segurança dos servidores, segurança em nuvem, entre outras.

9.2 Especializações aplicável: governança de segurança e continuidade de negócios, modelagem de ameaças, auditoria de segurança, tecnologias de firewall, Active Directory, gerenciamento de vulnerabilidades, testes de penetração, Microsoft 365 Defender XDR, investigação de ameaças com KQL, segurança de aplicativos na nuvem, Hacking Ético, tratamento de incidentes de segurança cibernética/informação, investigações forenses, engenharia SIEM e monitoramento SOC.

10. Limitações e Condições

Anexos do Acordo de Sede da COP 30

10.1. Os funcionários do Governo não deverão possuir de uma conta de rede ou de sistema com privilégios administrativos, a menos que expressamente autorizado por escrito pela Secretária Executiva.

10.2. O Governo não conservará nem transmitirá a terceiros quaisquer informações sensíveis recolhidas no contexto das reuniões pré-sessões/Conferências.

Apêndice: síntese das fases de implementação dos Serviços de segurança cibernética

Fases	**Descrição das fases**
Pré-conferência e prova de conceito (POC)	- Workshops - Perfil das ameaças e Avaliação dos Riscos - Auditoria do projeto de rede, imagens de computadores portáteis, soluções de impressão, componentes de rede e sistemas de firewall - Avaliação da segurança dos dispositivos móveis - Teste de penetração de sites Web de Conferências selecionados - Fornecimento de SIEM e solução de monitoramento de inventário / ativos - Informação contínua relativa a ameaças e riscos à segurança cibernética - Avaliação do local físico das TI e dos ativos relacionados com TI
Apoio pré-sessão e conferência	- Apoio operacional no local e prestação de relatórios diários - Prestação de resposta e gestão de incidentes de segurança informática - Monitoramento das atividades de redes sociais relacionadas com a COP 30 - Prestação de apoio cibernético forense, conforme necessário
Apoio pós-conferência	- Desativação e higienização de componentes de rede relacionados à segurança de TI