Universidade de Brasília

Boletim de Atos Oficiais da UnB em 16/10/2019
DOU de 16/10/2019, seção 2, página 3

ATO DO(A) DIRETORIA DO CENTRO DE INFORMÁTICA (DIR) Nº 41/2019

Institui a Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR da Universidade de Brasília – UnB e dá outras providências.

O DIRETOR DO CENTRO DE INFORMÁTICA (CPD) DA UNIVERSIDADE DE BRASILIA, no uso de suas atribuições e competências que lhe confere o Ato da Reitoria n° 1.219, considerando a recomendação do Comitê de TI da Universidade de Brasília CTI - UnB, em sua 1ª reunião extraordinária de 2019, considerando a Resolução da Câmara de Planejamento e Administração – CPLAD/UnB nº 004/2018, que institui a Política de Segurança da Informação e Comunicação da Universidade de Brasília – PoSIC/UnB, segundo o disposto na Instrução Normativa nº 1 do Gabinete de Segurança Institucional da Presidência da República, na Norma Complementar nº 05/IN01/DSIC/GSIPR, na Norma Complementar nº 08/IN01/DSIC/GSIPR, na Norma Complementar n° 20/IN01/DSIC/GSIPR e na Norma Complementar n° 21/IN01/DSIC/GSIPR,

Resolve,

Art. 1º Instituir a Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR da Universidade de Brasília – UnB, subordinada ao Centro de Informática – CPD, observando as diretrizes estabelecidas na Política de Segurança da Informação e Comunicações – PoSIC da UnB.

Art. 2º Para efeitos desta Instrução, foram adotadas as seguintes definições:

I – Agente Responsável: Servidor Público, ocupante de cargo efetivo da Universidade de Brasília, incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais;

II – Aquisição de evidência: processo de coleta e cópia das evidências relacionadas a incidente de segurança em redes computacionais;

III – Artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

IV – Coleta de evidências de segurança em redes computacionais: processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Este processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente;

V – Comunidade ou público alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes cibernéticos;

VI – CTIR GOV: Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do gabinete de Segurança Institucional da Presidência da República – GSI;

VII – Detecção de intrusão: é o serviço que consiste na análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar, mediante autorização, os procedimentos de resposta a incidentes de segurança em redes computacionais, com base em eventos com caraterísticas pré-definidas, que possam levar a uma possível intrusão e, ainda, possibilitar envio de alerta em consonância com o padrão de comunicação previamente definido entre ETIR da UnB e o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR GOV;

VIII – Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR: grupo de pessoas com responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes cibernéticos;

IX – Evidência digital: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento;

X – Incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XI – Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

XII – Log ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

XIII – Preservação de evidência de incidentes cibernéticos: é o processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações;

XIV – REDUnB – Rede de Dados da Universidade de Brasília: rede de computadores e serviços de tecnologia da informação e comunicação da Universidade de Brasília;

XV – Serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade;

XVI – Tratamento de artefatos maliciosos: é o serviço que consiste em receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa. Uma vez recebido, o mesmo deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou pelo menos sugerida, uma estratégia de detecção, remoção e defesa;

XVII – Tratamento de incidentes cibernéticos: é o serviço que consiste em receber filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências; e

XVIII – Tratamento de vulnerabilidades: é o serviço que consiste em receber informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção.

Art. 3º É missão da ETIR prestar o serviço de tratamento de incidentes cibernéticos com o objetivo de conter, tratar, responder, erradicar e orientar sobre o incidente de segurança da informação e comunicação na Rede de Dados da UnB (REDUnB) em tempo compatível a sua natureza, visando assegurar a continuidade dos serviços de TIC para o alcance dos objetivos institucionais.

Art. 4º A Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR atuará nas atividades de resposta a incidentes de segurança da informação na REDUnB, provendo atendimento para as diversas unidades da UnB – acadêmicas e administrativas, distribuídas nos diversos câmpus e ao público externo nas questões relacionadas ao gerenciamento da segurança cibernética.

§1º A ETIR atenderá diretamente todas as unidades da UnB, seus usuários e solicitantes externos que registrarem eventos identificados como incidentes de segurança, preferencialmente, por meio de registro eletrônico.

Art. 5º A ETIR será estabelecida segundo o Modelo 1, da Norma Complementar n° 05, e será composta por servidores efetivos do quadro funcional do Centro de Informática – CPD com conhecimento, habilidades e experiência técnica compatíveis com a missão da Equipe, e que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes cibernéticos na REDUnB.

Art. 6° A ETIR será constituída por integrantes – titulares, suplentes e um Agente Responsável –, todos servidores e representantes de diversas áreas do Centro de Informática – CPD, atribuindo um caráter multidisciplinar para a equipe.

§ 1° Os integrantes serão indicados pelo Diretor do Centro de Informática – CPD e designados por meio de Ato do Diretor do CPD.

§ 2° A atuação dos integrantes, do Agente Responsável e dos integrantes por convocação, não terá natureza remuneratória e não ensejará quaisquer ônus para a UnB.

§ 3° Funcionará como um grupo de trabalho permanente, multidisciplinar, de atuação primordialmente reativa e não exclusiva.

§ 4º A dedicação às atividades proativas, assim como a atuação por convocação, deverá ser acordada entre o Agente Responsável e o respectivo gestor de cada integrante da ETIR.

Art. 7° O processo de tomada de decisão relacionado a incidentes de segurança da informação e comunicação na REDUnB, com repercussão interna, será exercido pelo Agente Responsável da ETIR com supervisão do Diretor do Centro de Informática – CPD.

Parágrafo único: as demais decisões de caráter mais sensível serão avaliadas pelo Diretor do Centro de Informática – CPD, consultando o Comitê de Tecnologia da Informação (CTI-UnB) e a Alta Administração, sempre que necessário para a situação exigida.

Art. 8º. A ETIR seguirá o modelo "Autonomia Compartilhada", conforme a Norma Complementar Nº 05/IN01/DSIC/GSIC/PR, trabalhando em conjunto com outros setores do Centro de Informática – CPD e demais unidades da Universidade de Brasília – UnB a fim de auxiliarem no processo de tomada de decisão envolvendo incidentes cibernéticos.

Art. 9° A ETIR desenvolverá os seguintes serviços:

I – Reativos:

a. tratamento de incidentes de segurança cibernéticos;

b. tratamento de artefatos maliciosos; e

c. tratamento de vulnerabilidades.

II – Proativos:

a. detecção de intrusão.

Art. 10. O processo de gerenciamento de incidentes cibernéticos orientará as ações da ETIR e contemplará:

I – Notificação do Incidente: o recebimento de notificações de incidentes permite à ETIR atuar como ponto central para articulação de soluções dos problemas provocados por incidentes cibernéticos mediante a coleta de atividades e incidentes reportados, análise das informações e correlação destas no âmbito da UnB. As informações podem ser utilizadas também para determinar tendências e padrões de atividades de ataques e para recomendar estratégias de prevenção adequadas para toda a Universidade;

II – Análise de Incidentes: esta atividade consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito da análise é identificar o escopo do incidente, sua extensão, sua natureza e quais os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação;

III – Suporte à Resposta a Incidentes: neste caso, a ETIR atua no processo de recuperação. Esse serviço é prestado por e-mail ou pela indicação de documentos que possam auxiliar no processo de recuperação. Essa atividade pode envolver a interpretação dos dados coletados e na recomendação de estratégias de contenção e recuperação;

IV – Coordenação na Resposta a Incidentes: nesta atividade, a ETIR coordena as ações entre os envolvidos em um incidente, o que pode incluir redes e outros centros de tratamento (CSIRTs) externos ao seu âmbito de atuação. O processo envolve a coleta de informações de contato, a notificação dos responsáveis pelas redes, computadores ou sistemas que possam estar envolvidos ou comprometidos e a geração de indicadores e estatísticas relativas aos incidentes;

V – Distribuição de Alertas, Recomendações e Estatísticas: esta atividade consiste em disseminar informações relativas a novos ataques ou tendências de ataques observadas pela ETIR, por outros centros de tratamento. Alertas de incidentes, em geral, são produzidos pelo próprio CTIR Gov, baseados nas notificações recebidas ou em incidentes tratados, ou são redistribuições de alertas emitidos por outros Centros com responsabilidade nacional. O Centro de

Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov, ao redistribuir alertas, pode acrescentar recomendações específicas para seu público e atribuir diferentes graus de severidade.

Art. 11. Compete ao Diretor do Centro de Informática – CPD:

I – emitir Ato formalizando a criação da ETIR;

II – coordenar a preparação da infraestrutura necessária à equipe de tratamento de incidentes e resposta a incidentes cibernéticos na REDUnB;

III – designar ou destituir o Agente Responsável e/ou os membros que comporão a ETIR;

IV – criar, revisar, aprovar, revogar, divulgar as definições das atribuições e das responsabilidades dos membros da ETIR, além das normas, dos processos e dos subprocessos que orientarão as atividades e os trabalhos da Equipe;

V – acompanhar as investigações e as avaliações dos danos decorrentes de quebras e violações de segurança da informação;

VI – revisar e submeter às instâncias superiores, para análise e aprovação, as estratégias e os processos de tratamento e resposta a incidentes cibernéticos e os processo de coleta e preservação de evidências propostos pela ETIR e pela área de segurança do Centro de Informática – CPD;

VII – encaminhar os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação à Alta Administração e ao Comitê de Tecnologia da Informação da UnB (CTI), e quando for o caso, remissão ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR GOV;

VIII – interagir com os CSIRTs de Coordenação (Grupos de Coordenação de Resposta a Incidentes Cibernéticos) de acordo com os protocolos estabelecidos pela UnB;

IX – prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos integrantes da Equipe; e

X – administrar os indícios de ilícitos criminais no que se refere a incidentes cibernéticos, formalizando e comunicando à autoridade máxima da UnB para a adoção dos procedimentos legais julgados necessários com base nos normativos de segurança da informação estabelecidos no âmbito do Governo Federal e da UnB.

§ 1° Extraordinariamente, o Diretor do Centro de Informática – CPD poderá convocar adicionalmente representantes de outras unidades da Universidade de Brasília – UnB para atuarem no tratamento e resposta de determinado incidente cibernético.

§ 2° Quando conveniente e necessário, o Diretor do CPD autorizará a ETIR iniciar, por conta própria, o tratamento e resposta a determinadas classes de incidentes, devidamente caracterizadas e exemplificadas, seguidas dos limites de atuação, ou de comando para atuação, no processo de contorno, contenção ou solução dos respectivos incidentes classificados.

Art. 12. Compete ao Agente Responsável:

I – coordenar e gerenciar as atividades da ETIR, inclusive as atividades de caráter proativo para cumprimento da missão;

II – distribuir tarefas para a equipe;

III – elaborar e manter atualizado os processos e procedimentos internos da ETIR;

IV – utilizar a metodologia e as melhores práticas reconhecidas e recomendadas em instruções normativas em relação ao processo tratamento e resposta a incidentes cibernéticos e no processo de coleta e preservação de evidências para fins forenses e de conformidade à legislação do Governo Federal;

V – avaliar e definir ferramental tecnológico de apoio técnico-gerencial;

VI – definir e aplicar metodologias e ferramentas reconhecidas e recomendadas em referenciais técnicos no processo tratamento e resposta a incidentes cibernéticos e no processo de coleta e preservação de evidências;

VII – auxiliar na elaboração do processo, da metodologia e da norma de gerenciamento de incidentes cibernéticos;

VIII – identificar as necessidades de capacitação e, se necessário, treinar os integrantes da ETIR;

XI – interfacear a comunicação com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR GOV, ETIR de outros órgãos da Administração Pública Federal e com o Centro de Atendimento a Incidentes de Segurança – CAIS/RNP; e

X – auxiliar o Diretor do Centro de Informática com subsídios informacionais para a tomada de decisão relativa a incidentes cibernéticos.

Parágrafo único: extraordinariamente, o Agente Responsável poderá convocar adicionalmente representantes de outros setores do Centro de Informática – CPD para atuarem no tratamento e resposta de determinado incidente cibernético.

Art. 13. Compete aos membros da ETIR:

I – agir proativamente com o objetivo de evitar que ocorram incidentes de segurança da informação, divulgando práticas e recomendações, avaliando as condições de segurança da REDUnB por meio de verificações sistêmicas de conformidade e identificação de vulnerabilidades e artefatos maliciosos;

II – realizar ações reativas que incluem recebimento de notificações de incidentes cibernéticos, atuando no reparo aos danos causados e no restabelecimento dos serviços de tecnologia da informação e comunicação e sistemas comprometidos, investigando e analisando as causas, danos e responsáveis, recomendando procedimentos a serem executados ou as medidas de recuperação a serem adotadas durante um incidente de segurança;

III – disponibilizar relatórios gerenciais em períodos previamente definidos ou quando solicitados pelo Diretor do CPD ou pelo Agente Responsável;

VI – cooperar com outras Equipes de Tratamento e Resposta a Incidentes cibernéticos ou equipes equivalentes de segurança da informação de acordo com os protocolos de cooperação estabelecidos pela UnB;

V – manter contato com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSI/PR e com o CTIR Gov – Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo concernente a assuntos de segurança cibernética;

VI – participar de eventos relativos à segurança da informação e incidentes cibernéticos; e

VII – subsidiar o Agente Responsável, o Diretor do Centro de Informática – CPD e o Comitê de TI da UnB (CTI – UnB) com informações e evidências coletadas em apurações quando da suspeita de ocorrências de quebras de segurança e/ou violações de segurança da informação e comunicação.

Art. 14. Os incidentes de segurança cibernéticos na Rede de Dados da Universidade de Brasília – REDUnB devem ser notificados e comunicados pelos usuários dos serviços de TI da UnB e agentes internos e externos por meio dos canais:

I – e-mail: abuse@unb.br;

II – serviço web: http://etir.unb.br;

III – pessoalmente – em casos emergenciais; e

IV – por intermédio de ferramental tecnológico e eventos de risco detectados pelo monitoramento de segurança.

Art. 15. A Norma que disciplina o gerenciamento de incidentes de segurança da informação e do registro de eventos, coleta e preservação de evidências de incidentes cibernéticos no âmbito da Universidade de Brasília versará, dentre outras diretrizes inerentes, sobre os serviços a serem prestados pela ETIR.

Art. 16. Assim que possível, e considerando a determinação e realidade da UnB, a implementação da ETIR deverá ser migrada para o modelo "2 - Centralizado", conforme Norma Complementar Nº 05/IN01/DSIC/GSIC/PR.

Art. 17. Este documento deverá ser revisado periodicamente, em intervalos de até dois anos, ou quando necessário.

Art. 18. Este Ato entra em vigor na data de sua publicação.

Brasília, 15 de outubro de 2019

CENTRO DE INFORMÁTICA

Documento assinado eletronicamente por **Jacir Luiz Bordim**, **Diretor(a) do Centro de Informática**, em 15/10/2019, às 20:50, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4541314** e o código CRC **F319F79F**.

Referência: Processo nº 23106.131319/2019-11 SEI nº 4541314