

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA



SALVADOR, 06 de setembro de 2022.

Of. nº TJ-OFI-2022/06478

Excelentíssimo Senhor
Desembargador Mário Albiani Júnior
Diretor-Geral da Universidade Corporativa TJBA
Assunto: Solicitação de treinamento

Excelentíssimo Des. Diretor-Geral da UNICORP,

Com meus respeitosos cumprimentos, solicito os valiosos préstimos dessa Universidade Corporativa a fim de promover a contratação de capacitação para nove servidores da área de tecnologia da informação em segurança cibernética, incluindo temas como defesa cibernética, como atuar em caso de incidentes e como pensar como um hacker.

Os treinamentos de segurança e cibersegurança seguem determinação do Conselho Nacional de Justiça(CNJ), por meio de sua Resolução nº 396, de 7 de junho de 2021, a qual instituiu a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ). Outrossim, o Manual de Referência de Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário, disponível em <https://www.cnj.jus.br/wp-content/uploads/2021/03/AnexoVIIManualReferenciaPoliticaDeEducacaoCulturaSegurancaInformacaoRevisadoREV.docx.pdf>, estabelece que servidores da área de Tecnologia da Informação e Comunicação e de Segurança da Informação devem estar qualificados em segurança cibernética em nível de graduação, pós-graduação ou de certificações especializadas, devendo, ainda, serem promovidos treinamentos específicos, para que sejam capazes de entender como e quais são as melhores práticas globalmente adotadas para minimizar os possíveis impactos causados por um ciberataque.

Nesse sentido, a capacitação proposta é composta de três cursos, conforme descrição detalhada a seguir: Treinamento do programa CND (Certified Network Defender), que visa preparar o servidor em tecnologias de segurança de rede e operações para atingir Defense-in-Depth (defesa de profundidade); Treinamento EC-Council Certified Incident Handler, que visa preparar os técnicos para lidarem com possíveis consequências pós-ataque e o Certified Ethical Hacker (CEH), que objetiva ensinar como os hackers pensam e agem maliciosamente para que a instituição esteja preparada em caso de ataque.

1) Treinamento do programa CND (Certified Network Defender)

Programa de treinamento de certificação de *vendor* neutro, com 40 horas de aulas online, baseado em competências, com laboratórios práticos, focados nas principais ferramentas de segurança de rede e técnicas que fornecerão aos administradores de rede experiência do mundo real em tecnologias e operações atuais de segurança, para que possam detectar e responder à abordagem de segurança de rede. Visa, ainda, preparar os administradores de rede em tecnologias de segurança e operações para atingir Defense-in-Depth (defesa de profundidade) e foi mapeado para papéis de trabalho globais e responsabilidades, sendo adotado pelo Departamento de Defesa (DoD) dos Estados Unidos.

2) Treinamento EC-Council Certified Incident Handle

Após um desenvolvimento rigoroso que incluiu uma Análise de Tarefa de Trabalho (JTA) cuidadosa relacionada ao tratamento de incidentes e trabalhos de resposta a incidentes, o EC-Council desenvolveu um programa de treinamento intensivo altamente interativo, abrangente, com uma imersão de três dias em aulas práticas, com carga horária de 24 horas online (ao vivo), em nível especialista, que transmite conhecimentos e habilidades necessárias para que se possa lidar com as consequências pós-violação, reduzindo o impacto



PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA

do incidente, tanto do ponto de vista financeiro quanto de reputação.

Assim, busca garantir que a organização possa identificar, conter e recuperar-se de um ataque, reintegrando as suas operações regulares o mais cedo possível e mitigando o impacto negativo nas operações de negócios. Ademais, auxiliará no desenvolvimento de competências para elaborar políticas de segurança com eficácia para minimizar a perda e a violação de efeitos posteriores a ocorrência de incidente.

3) Treinamento Certified Ethical Hacker (CEH) Version 12

O International Council of E-Commerce Consultants (EC-Council) é uma organização internacional com base em Nova Iorque, líder mundial em certificações e treinamentos de segurança eletrônica, dedicada ao desenvolvimento de cursos e à distribuição de certificações na área de Segurança da Informação e Comércio Eletrônico,

O curso com carga horária de 40 horas, com aulas online (ao vivo), visa fornecer uma compreensão aprofundada das fases de hacking ético, de vários vetores de ataque e contramedidas preventivas, com o objetivo de ensinar como os hackers pensam e agem maliciosamente para que a instituição possa melhor configurar sua infraestrutura de segurança e defender-se de ataques futuros. Compreender os pontos fracos e vulnerabilidades do sistema ajuda a intuição a fortalecer seus controles de segurança de sistema para minimizar o risco de um incidente.

Conforme exposto, a capacitação compreende o total de 104 horas de treinamento em matérias especializadas em segurança da informação, visando aprimorar os conhecimentos técnicos dos servidores, buscando assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações, notadamente dos processos judiciais e administrativos deste Poder Judiciário. Para atendimento foram colhidas duas propostas de empresas credenciadas à organização de segurança, ora anexadas a este expediente. Ambas as empresas selecionadas possuem profissionais especializados e com vasta experiência em segurança da informação e cibersegurança.

Certo de contar com o apoio de Vossa Excelência, aproveito o ensejo para renovar votos de estima e distinta consideração.

RICARDO NERI FRANCO
SECRETÁRIO TECNOLOGIA DA INFORMAÇÃO E MODERNIZAÇÃO

