



Año 2022 – “Las Malvinas son argentinas”

RESOLUCIÓN C.S.N° : 326/2022

Avellaneda, Pcia. de Buenos Aires

VISTO:

El Expediente Electrónico N°1165/2022, la Resolución C.S. N°151/2018; y

CONSIDERANDO:

Que la Universidad Nacional de Avellaneda tiene como misión primaria la construcción, recuperación, conservación y generación de conocimiento, con el objeto de difundirlo, transferirlo y aplicarlo a la sociedad, a fin de dar respuesta a sus preocupaciones, necesidades y demandas, y propiciar la mejora de sus condiciones de vida, en el marco de un desarrollo sustentable.

Que por Resolución C.S. N°151/2018 se aprobó la creación del “Programa de Formación en Oficios” en el marco de la Secretaría de Extensión Universitaria.

Que la Secretaria de Extensión Universitaria, Lic. Liliana Elsegood, eleva al Consejo Superior para su tratamiento y aprobación el desarrollo del curso “Seguridad Informática Básico”.

Que el mismo fue elaborado por profesionales de la carrera de Ingeniería en Informática y coordinado con el Programa de Formación en Oficios de la Secretaría de



Año 2022 – “Las Malvinas son argentinas”

Extensión Universitaria de la Universidad Nacional de Avellaneda.

Que habiéndose puesto en consideración de los Consejeros la procedencia del dictado del acto administrativo que apruebe el desarrollo del curso mencionado, sin mediar objeciones, resulta aprobado por unanimidad en la Sesión N°CI el requerimiento que motiva las presentes actuaciones.

Que la Comisión Permanente de Enseñanza e Investigación del Consejo Superior ha tomado la intervención que le compete proponiendo el dictado de la presente resolución.

Que se ha expedido la Abogada dictaminante.

Que la presente se dicta contando con la plena conformidad de los integrantes del Consejo Superior, y en pleno uso de las facultades atribuidas a través del Estatuto Universitario en su artículo 39.

POR ELLO,

EL CONSEJO SUPERIOR DE LA UNIVERSIDAD NACIONAL DE AVELLANEDA

RESUELVE:

ARTÍCULO N°1: Aprobar el desarrollo del curso “Seguridad Informática Básico”, conforme a los marcos de referencia, cuyo ANEXO I forma parte integral de la presente resolución.

ARTÍCULO N°2: Delegar en la Secretaría de Extensión Universitaria las gestiones relativas a la ejecución y la expedición de los certificados correspondientes.



Año 2022 – “Las Malvinas son argentinas”

ARTICULO N°3: Regístrese. Comuníquese a la Secretaría de Extensión Universitaria, a la Secretaría de Consejo Superior y al Departamento de Tecnología y Administración. Cumplido, archívese.

RESOLUCIÓN C.S. N°: 326/2022

Secretario de
Consejo Superior

Presidente de
Consejo Superior

ANEXO I**“Seguridad Informática Básico”****Introducción:**

La información es uno de los activos más importantes que tienen las organizaciones. Con los avances tecnológicos permanentes, ésta se procesa y almacena en sistemas informáticos.

Estos sistemas, pueden ser vulnerables y, por lo tanto, estar expuestos a riesgos y amenazas. Por este motivo, es fundamental que se realicen controles permanentes que permitan un funcionamiento eficiente y seguro.

Perfil del egresado/a:

El/la egresado/a del curso será capaz de desarrollar las técnicas y los mecanismos básicos para proteger servidores, estaciones de trabajo y dispositivos.

Contenidos:

Unidad Temática I: Introducción a la seguridad informática.

Fundamentos de la Seguridad Informática. Navegación Segura: Permisos de Usuarios. Permisos de Grupos. User Account Control (UAC) Carpetas Compartidas Backup. Recuperación. Seguridad Windows: Introducción. Local Security Policy Política de Contraseñas Introducción.



Año 2022 – “Las Malvinas son argentinas”

Software Restriction Policy AppLocker. Criptografía: Introducción Hashes Introducción Cracking de Hashes. On The Fly Encryption Gestión de Contraseñas. Malware: Introducción Ejemplos de Malware Software Antimalware. Introducción. Servicios de Análisis Online Ransomware.

Módulo II: Introducción a redes.

Componentes y tipos de redes. Tipos de topologías. Elementos que componen una red. Ancho de banda y medios de acceso. Especificaciones Ethernet Estándar de cableado UTP. Medio de fibra óptica. Medio inalámbrico. Protocolo de aplicaciones. Protocolo de red. Protocolo de transporte. Protocolo de internetworking. Estándar OSI. Diferencias y similitudes entre el modelo OSI y el modelo Internet. Servicios de DNS, DHCP, WWW y FTP. 4. Estándar Ethernet. Estructura de una trama Ethernet Uso y función de Gateway. Estructura de una red IPv4. Estructura de una red IPv6. Máscara de subred y su influencia en TCP/IP Distintos entes reguladores y sus funciones. Capa de transporte, VPN y acceso inalámbrico. Protocolo de datagramas de usuario (UDP). Protocolo de control de transmisión (TCP). Direccionamiento de puertos. Tecnología VPN Distintos accesos de VPN.

Módulo III: Introducción a base de datos y SQL.

Introducción a Bases de Datos. Entorno MySQL. MySQL como sistema de administración relacional de bases de datos. Crear, eliminar y utilizar una base de datos. Concepto de Entidad, atributo y tipo de datos Restricciones Primary Key, Not Null, Default Inserción

de Datos. Lenguaje SQL: Estructura de una consulta SQL. Cláusula SELECT. Alias Literales. Cláusula FROM. Predicado (Cláusula WHERE) Operadores de comparación Operadores lógicos (AND - OR) Sentencias (BETWEEN - IN - LIKE). Ordenación. Manipulación de datos: Eliminación de registros Actualización de registros Funciones de agregado Agrupamiento. Predicado HAVING. Tópicos Avanzados: Concepto de relación Restricción Foreign Key. Concepto de Integridad Referencial. Consultas relacionando distintas tablas a través de INNER JOIN.

Módulo IV: Criptografía y blockchain.

Criptografía Clásica: Conceptos generales Transposición Sustitución. Historia Criptoanálisis. Principios de Kerckhoff. Criptografía Simétrica y Asimétrica: Criptografía Simétrica Conceptos. Tipos de Criptografía Simétrica Bloque. Flujo Problemáticas OpenSSL. Criptografía Asimétrica Conceptos. Usos de la Criptografía Asimétrica Cifradores. Generadores de claves Curvas Elípticas. Firma electrónica vs Firma digital OpenSSL. GnuPG. HASH y otras aplicaciones Criptográficas: HASH. Conceptos Colisiones. Ataque de cumpleaños Rainbow tables, HMAC. Cifrado al Vuelo. Conceptos Usos comunes VeraCrypt Esteganografía Conceptos. Aplicación. Infraestructura de Clave Pública: Conceptos Arquitectura Implementación Usos Problemáticas Blockchain. ¿Qué es la Blockchain? Criptomonedas Árbol de Merkle. Redes P2P. Consenso. Minería. Otras Aplicaciones.

Módulo V: Seguridad en Windows - server hacking.

Local Security Policy: Local Security Policy Política de Contraseñas. Política de Bloqueo de Cuentas Software Restriction Policy AppLocker. Eventos y Auditoría: Windows Event Log Política de Auditoría. Política de Auditoría Avanzada Process Monitor (procmon). System Monitor (sysmon). Post-Explotación I: Post Explotación. Técnicas Living of the Land Elevación de Privilegios. Saltar User Account Control con UACME Saltar User Account Control manualmente. Post Explotación II: Windows Exploit Suggester Next Generation (WES-NG) Explotación de CVE-2019-1322 + CVE-2019-1405 con COMahawk Abuso de Servicios por Permisos Vulnerables. Abuso de Servicios con binPath Vulnerable Abuso de Servicios Utilizando DLL Hijacking. Volcado de Hashes desde el Registro de Windows Mimikatz. Volcado de Memoria LSASS. Acceso a Credenciales en Memoria Pass The HashCapacidades referentes al perfil profesional que se abordan en el módulo.

Módulo VI: Desarrollo seguro.

Fundamentos de la Seguridad Informática: Tríada CID (Confidencialidad, Integridad, Disponibilidad) Términos de Interés (Amenaza, Vulnerabilidad, Riesgo, etc.) Estándares de Interés (ASVS, CWE, CVSS, etc.) Separación de Ambientes. OWASP Top 10. Proactive Controls Configuración de Herramientas del Laboratorio



Año 2022 – “Las Malvinas son argentinas”

C1: Define Security. Requirements. C2: Leverage Security Frameworks and Libraries C3: Secure Database. Access. Datos Fiables vs Datos No Fiables: C4: Encode and Escape Data C5: Validate. All Inputs. Laboratorio Cross Site Scripting (XSS). Laboratorio Command Injection. C6: Implement Digital Identity: Autenticación. Factores de Autenticación Algo que sé, algo que tengo, algo que soy. Autenticación Multi-Factor (MFA) Laboratorio Autenticación. Multi-Factor Sesiones. Laboratorio Sesiones. C7: Enforce Access Controls. C8: Protect. Data Everywhere: Criptografía. Algoritmos Criptográficos Recomendados. C9: Implement Security Logging and Monitoring C10: Handle all Errors and Exceptions. Laboratorio de Análisis de Código.

Carga horaria: 80hs

RESOLUCIÓN C.S. N°: 326/2022

Secretario de
Consejo Superior

Presidente de
Consejo Superior