

REPÚBLICA DEL PERÚ



Resolución de Presidencia del Consejo Directivo Ad Hoc

N° 330-2017-SINEACE/CDAH-P

Lima, 17 AGO. 2017

VISTO:

El Informe N° 036-2017-SINEACE/P-DEC-IEES, emitido por la Dirección de Evaluación y Certificación de Institutos y Escuelas de Educación Superior; y,

CONSIDERANDO:

Que, el artículo 5° de la Ley N° 28740, Ley del Sineace establece como finalidad del Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa, garantizar a la sociedad que las instituciones educativas públicas y privadas ofrezcan un servicio de calidad, con el propósito de optimizar los factores que incidan en los aprendizajes y en el desarrollo de las destrezas y competencias necesarias para alcanzar mejores niveles de calificación profesional y desarrollo laboral;

Que, mediante la Décima Segunda Disposición Complementaria Transitoria de la Ley N° 30220, Ley Universitaria, se declara en reorganización el Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa – Sineace, habiéndose conformado mediante Resolución Ministerial N°396-2014-MINEDU, del 28 de agosto 2014, el Consejo Directivo Ad Hoc, con el objetivo de ejecutar las funciones necesarias para la continuidad del sistema y los procesos en desarrollo;

Que, mediante el documento de visto, la Dirección de Evaluación y Certificación de Institutos y Escuelas de Educación Superior, propone la aprobación de las siguientes normas que cumplen con la validación de expertos y la demanda del mercado laboral:

1. Normas de Competencias en el Sector Información y Comunicaciones, Familia Productiva Tecnología de la Información y Comunicaciones – TICs:
 - a. Normas de Competencia del Profesional Técnico en Análisis de Sistemas
 - b. Normas de Competencia del Profesional Técnico en Redes y Seguridad Informática.
2. Normas de Competencias en el Sector Explotación de Minas y Canteras, Familia Minería Metálica:
 - a. Normas de Competencia del Profesional Técnico en Explotación Minera.

Que, en ejercicio de las facultades otorgadas al Consejo Directivo Ad Hoc del Sineace, en sesión de fecha 02 de agosto 2017, mediante los siguientes acuerdos aprobó:



- **Acuerdo N° 243-2017-CDAH:** Aprobar el documento técnico denominado Normas de Competencia del Profesional Técnico en Análisis de Sistemas.
- **Acuerdo N° 244-2017-CDAH:** Aprobar el documento técnico denominado Normas de Competencia del Profesional Técnico en Redes y Seguridad Informática.
-
- **Acuerdo N° 245-2017-CDAH:** Aprobar el documento técnico denominado Normas de Competencia del Profesional Técnico en Explotación Minera.

De conformidad con la Ley N° 28740, Ley del Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa – Sineace, su Reglamento aprobado con Decreto Supremo N° 018-2007-ED, la Ley N° 30220 Ley Universitaria; Resolución Ministerial N° 396-2014-MINEDU y modificatorias; y la Resolución Ministerial N° 331-2017-MINEDU;

SE RESUELVE:

Artículo 1°. - Oficializar los Acuerdos N° 243-2017-CDAH, N°244-2017-CDAH y N°245-2017-CDAH, de sesión de fecha 02 de agosto 2017, mediante los cuales el Consejo Directivo Ad Hoc aprobó los documentos técnicos denominados: *Normas de Competencia del Profesional Técnico en Análisis de Sistemas*, *Normas de Competencia del Profesional Técnico en Redes y Seguridad Informática*; y *Normas de Competencia del Profesional Técnico en Explotación Minera*, respectivamente, que en anexo forma parte integrante de la presente resolución.

Artículo 2°. - Disponer la publicación de la presente resolución en el Diario Oficial El Peruano, así como en el Portal Web del Sineace.

Regístrese, comuníquese y publíquese.



Carolina Barrios Valdivia

CAROLINA BARRIOS VALDIVIA
Presidenta del Consejo Directivo Ad Hoc
Sineace

SERIE DE DOCUMENTOS TÉCNICOS

NORMAS DE COMPETENCIA
DEL PROFESIONAL TÉCNICO
EN REDES Y SEGURIDAD INFORMÁTICA



INCLUYE LOS
APORTES DE LOS
PARTICIPANTES

Consejo Directivo Ad hoc

Peregrina Morgan Lora, Presidenta

Gisella Orjeda Fernández

Jorge Víctor Zegarra Pellanne

Secretaría Técnica:

Carolina Barrios Valdivia

Dirección de Evaluación y Certificación

Luisa Esther Ramos Yllescas, Directora

Benedícta Brígida Huaytalla Tenio

Silenia Yesenia Rodríguez Córdova

Teresa Mercedes Salas Aquije

Nancy Amparo Vera Junchaya

Cuidado de la edición

Centro de Información y Referencia

César Arriaga Herrera, Coordinador

Oficina de Comunicaciones

Diseño y Diagramación

Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa

Calle Manuel Miota 235, Urb. San Antonio, Miraflores, Lima 18, Perú

Teléfonos: (51-1) 221-4826, (51-1) 2214807 anexo 108

E-mail: cir@sineace.gob.pe/www.sineace.gob.pe

INDICE

1. PRESENTACION	5
2. INTRODUCCION	6
3. ALCANCE	7
4. BASE LEGAL	7
5. MAPA FUNCIONAL	8
6. UNIDADES DE COMPETENCIA	
UNIDAD DE COMPETENCIA N° 1:	9
UNIDAD DE COMPETENCIA N° 2:	12
UNIDAD DE COMPETENCIA N° 3:	16
7. ANEXO	21

PRESENTACIÓN

La Seguridad Informática ha experimentado un profundo cambio en los últimos años. Inversiones aisladas llevadas a cabo con el objetivo de fortalecer la seguridad en puntos muy concretos han dado paso a inversiones para asegurar el bien más valioso de la empresa, la información, enfocando la seguridad hacia los procesos de negocio de la empresa.

Durante los años 80 y principios de los 90 la Seguridad Informática se centraba en proteger los equipos de los usuarios, es decir, proporcionar seguridad a los ordenadores y su sistema operativo. Esta seguridad lógica, entendida como la seguridad de los equipos informáticos para evitar que dejasen de funcionar correctamente, se centraba en la protección contra virus informáticos.

Con la aparición de Internet y su uso globalizado a nivel empresarial la Seguridad Informática comenzó a enfocarse hacia la conectividad de redes o networking, protegiendo los equipos servidores de aplicaciones informáticas, y los equipos servidores accesibles públicamente a través de Internet, y controlando la seguridad a nivel periférico a través de dispositivos como Firewalls. Es decir, la posibilidad tecnológica de "estar conectados" llevaba implícita la aparición de nuevas vulnerabilidades que podían ser explotadas, la exposición de información crucial para el negocio que podía ser accesible precisamente gracias a esa conectividad. (Evolución de la seguridad informática. Disponible: <https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica>)

Bajo esta premisa y derivado del crecimiento que tienen las empresas en el Perú se ha ido acrecentando la inseguridad a todo nivel de las empresas, haciendo que las organizaciones busquen tener la mayor seguridad en sus programas. El futuro está marcado por la seguridad informática, y el desarrollo de esta área está creando especialidades como la de redes y seguridad informática, en un mundo globalizado de negocios digitales. En este contexto, es que SINEACE ha priorizado la normalización de la profesión técnica en Redes y Seguridad Informática como un aporte al desarrollo y crecimiento de las empresas.

INTRODUCCIÓN

EL Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa (SINEACE) pone a disposición de las instituciones, profesionales técnicos interesados y público en general, las Normas Técnicas para la Certificación de Competencias del Profesional Técnico en Redes y Seguridad Informática, como producto de las comisiones técnicas con actores involucrados en el sector.

Estas normas tienen por objetivo establecer estándares de calidad para la certificación de competencias profesionales de personas con formación técnica en Instituciones y Escuelas de Educación Superior Tecnológicas No Universitarias. La finalidad es garantizar a las instituciones y empresas del sector involucrado personal capacitado para realizar idóneamente las funciones y actividades propias de la actividad de gestión de redes y seguridad informática, considerando criterios acordes a estándares internacionales vigentes.

Estas normas han sido elaboradas con la participación de empresarios, trabajadores y académicos de la profesión y constituyen una de las herramientas fundamentales para que las Entidades Certificadoras autorizadas efectúen procesos de certificación rigurosa, transparente y de calidad conforme a las disposiciones que regulan su funcionamiento.

Con la publicación de estas normas, se reitera la apuesta por la mejora de la calidad educativa y el desarrollo del país fomentando una cultura evaluadora permanente y continua. A su vez, expresa la disposición del SINEACE para seguir mejorando su quehacer con la participación de la ciudadanía y entidades interesadas.

Alcance

El presente documento es de aplicación a nivel nacional y está dirigido a:

- Egresados y titulados de los Institutos y Escuelas de Educación Superior Tecnológica.
- Egresados y titulados de otros Institutos y Escuelas de Educación Superior No Universitaria que tienen la facultad de otorgar títulos a nombre de la nación.
- Entidades Certificadoras autorizadas.

Base legal

- Constitución Política del Perú.
- Ley N° 28044, Ley General de Educación, que regula la creación del Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa (artículos N° 14ª, 15ª y 16ª), promulgada el 28 de julio de 2003.
- Ley N° 28740, Ley del Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa.
- Decreto Supremo N° 018 – 2007 – ED Reglamento del SINEACE
- Ley No. 30220, Ley Universitaria

Unidades de competencia

Unidad de Competencia No. 1	
Programador de servicios e infraestructura de redes y la seguridad informática.	(Código 001)
Organizar los servicios e infraestructura de redes y la seguridad informática de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.	

Unidad de Competencia No. 2	
Programador de servicios e infraestructura de redes y sistemas de seguridad informática.	(Código 002)
Implementar servicios e infraestructura de redes y sistemas de seguridad informática de acuerdo al diseño y especificaciones técnicas según políticas de la organización (plan operativo).	

Unidad de Competencia No. 3	
Mantenimiento de la funcionalidad y seguridad de los servicios de redes y servicios de seguridad informática	(Código 003)
Mantener la funcionalidad y seguridad de los servicios de redes y servicios de seguridad informática, de acuerdo a los lineamientos establecidos por la organización.	

MAPA FUNCIONAL PROFESIONAL TÉCNICO EN REDES Y SEGURIDAD INFORMATICA

Propósito Principal	Unidades de Competencia	Elementos de Competencia
Gestionar, implementar y mantener la infraestructura física y lógica de redes y seguridad informática, de acuerdo a las políticas de la organización, normas y tecnologías vigente	1. Organizar los servicios e infraestructura de redes y la seguridad informática de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.	1.1. Identificar y diagnosticar el estado situacional de la red, de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
		1.2. Proponer los recursos físicos y lógicos de la red, de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
		1.3. Elaborar el plan de implementación de la red y seguridad informática, de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
	2. Implementar servicios e infraestructura de redes y sistemas de seguridad informática de acuerdo al diseño y especificaciones técnicas según políticas de la organización (plan operativo)	2.1. Ejecutar el plan de seguridad de la información en la infraestructura de redes y seguridad informática, de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
		2.2. Instalar dispositivos y servicios de red y seguridad informática, de acuerdo a normas vigentes.
		2.3. Configurar dispositivos y servicios de red y seguridad informática, de acuerdo a normas vigentes.
		2.4. Verificar la operatividad de los dispositivos y servicios instalados de acuerdo al plan de implementación.
	3. Mantener la funcionalidad y seguridad de los servicios de redes y servicios de seguridad informática, de acuerdo a los lineamientos establecidos por la organización.	3.1. Monitorear el funcionamiento de la infraestructura de redes y seguridad informática, de acuerdo a los lineamientos establecidos por la organización.
		3.2. Diagnosticar el estado de los dispositivos y servicios, de acuerdo a los lineamientos establecidos por la organización.
		3.3. Ejecutar el plan de mantenimiento preventivo y correctivo de la infraestructura de redes, seguridad y servicios de acuerdo a los lineamientos establecidos por la organización.
		3.4. Ejecutar el plan de respuesta a incidencias de redes y seguridad informática de acuerdo a los lineamientos establecidos por la organización.

UNIDAD DE COMPETENCIA N° 01

Programador de los servicios e infraestructura de redes y la seguridad informática

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMÁTICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-001-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	1 Organizar los servicios e infraestructura de redes y la seguridad informática de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-001-RSI-V1-2016-EC01
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	1.1 Identificar y diagnosticar el estado situacional de la red, de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
<p>ES COMPETENTE SI:</p> <p>A. El diagrama lógico y físico de la red y seguridad informática es elaborada de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.</p> <p>B. El software de análisis de vulnerabilidades es ejecutado de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes</p> <p>C. El desempeño de la infraestructura de redes y seguridad de la organización es medida de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.</p>	<p>DESEMPEÑO: Profesional técnico identificando y diagnosticando el estado situacional de la red.</p> <p>A. Elabora diagrama lógico y físico de la red y seguridad informática.</p> <ul style="list-style-type: none"> - Realiza inventario de activos informáticos y licencias. - Describe la distribución lógica de los componentes de red. - Determina la ubicación física de los equipos en la red - Realiza evaluación de riesgos sobre la red. - Elabora e interpreta diagramas de red <p>B. Ejecuta software de análisis de vulnerabilidades.</p> <ul style="list-style-type: none"> - Instala aplicaciones para la detección de vulnerabilidades y amenazas de red. - Ejecuta el software de análisis de vulnerabilidades y amenazas - Determina el alcance del análisis de vulnerabilidades y amenazas. <p>C. Mide el desempeño de la infraestructura de redes y seguridad de la organización.</p> <ul style="list-style-type: none"> - Identifica los parámetros que caracteriza el desempeño de los componentes de red y seguridad. - Mide los niveles de procesamiento, almacenamiento y memoria de los equipos tecnológicos. - Determina los umbrales de funcionamiento de los parámetros de los componentes de red y seguridad. <p>PRODUCTO:</p> <ul style="list-style-type: none"> - Documento matriz de riesgos y seguridad informática. - Diagrama lógico y físico de la red interna de la organización. - Inventario de activos informáticos. - Reporte de vulnerabilidades y amenazas. - Reporte del desempeño de la infraestructura de red <p>ACTITUDES:</p> <p>Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.</p>
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
<ol style="list-style-type: none"> 1. Simuladores de red. 2. Software de diagramación de redes. 3. Herramientas de análisis de vulnerabilidades y amenazas. 4. Ofimática. 5. Sistemas operativos. 6. Conocimientos de hardware de redes 7. Conocimientos de licenciamientos de sistemas operativos y seguridad informática 8. Conocimiento de redes y comunicaciones 9. Conocimiento de gestión de cambios relacionado al modelo ITIL 10. Conocimiento de las ISO 27000 y ISO 17799 	
CAMPO DE APLICACIÓN	
CATEGORIA:	CLASE:
<ol style="list-style-type: none"> 1. Método 2. Ambiente: 	<ol style="list-style-type: none"> 1.1. Manual 1.2. Automatizada 2.1. Centro de computo/Oficina

3. Equipos y herramientas:	3.1. Capturador de tráfico 3.2. Herramientas de análisis de vulnerabilidades y amenazas. 3.3. Herramienta de inventario de activos 3.4. Herramientas de testeo de red
-----------------------------------	--

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMÁTICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-001-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	1 Organizar los servicios e infraestructura de redes y la seguridad informática de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-001-RSI-V1-2016-EC02
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	1.2 Proponer los recursos físicos y lógicos de la red de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
ES COMPETENTE SI: <p>A. Las necesidades y problemática de la infraestructura de redes y seguridad informática son identificadas de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.</p> <p>B. Las soluciones a la problemática y necesidades detectadas de la infraestructura de redes y seguridad de la información son propuestas de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.</p>	DESEMPEÑO: El profesional técnico proponiendo los recursos físicos y lógicos de la red. <p>A. Identifica las necesidades y problemática de la infraestructura de redes y seguridad informática.</p> <ul style="list-style-type: none"> - Realiza pruebas de pentesting a la red (penetración a la red) - Identifica las necesidades de equipos de red y seguridad para satisfacer los requerimientos de la organización. - Identifica los problemas que no son cubiertos por la infraestructura actual. <p>B. Propone las soluciones a la problemática y necesidades detectadas de la infraestructura de redes y seguridad de la información.</p> <ul style="list-style-type: none"> - Determina las acciones a ejecutar para corregir los problemas detectados. - Propone la tecnología para cubrir las nuevas necesidades y problemas. - Determina el software y hardware para la solución <p>PRODUCTO: Propuesta técnica de soluciones de infraestructura interna, físicos y lógicos.</p> <p>ACTITUDES: Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.</p>
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
<ol style="list-style-type: none"> 1. Ofimática 2. Herramientas de redes y seguridad informática. 3. Conocimientos de hardware y software especializados en redes 4. Conocimientos de Data Networking 5. Conocimientos de electrónica básica 6. Conocimientos de ISO 27000 y ISO 17799 	
CAMPO DE APLICACIÓN	
CATEGORIA:	CLASE:
1. Método	1.1. Manual
2. Ambiente:	1.2. Automatizada
	2.1. Centro de computo
	2.2. Oficina
	2,3. Laboratorio piloto
3. Equipos y herramientas:	3.1. Capturador de tráfico
	3.2. Herramientas de análisis de vulnerabilidades y amenazas.
	3.3. Herramienta de inventario de activos

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMÁTICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-003-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	1. Organizar los servicios e infraestructura de redes y la seguridad informática de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-003-RSI-V1-2016-EC01
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	1.3 Elaborar el plan de implementación de la red y seguridad informática, acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
ES COMPETENTE SI: A. El Plan de implementación es elaborado de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes. B. El plan de implementación es organizado de acuerdo a las especificaciones técnicas según el plan operativo de la organización.	DESEMPEÑO: Profesional técnico elaborando el plan de implementación. A. Elabora plan de implementación. - Determina el alcance del plan de implementación - Determina los recursos (software, hardware y humanos) - Elabora cronograma de actividades. - Elabora plan de contingencias ante imprevistos B. Organiza el plan de implementación - Realiza lista de chequeo sobre las actividades o tareas involucradas en el plan de implementación. - Programa las fechas para las diferentes fases del plan - Determina las pruebas de verificación - Revisa los niveles de servicios de acuerdo a las necesidades de la empresa y los estándares vigentes. - Controla y ajusta los tiempos del plan. PRODUCTO: Plan de implementación. ACTITUDES: Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
<ol style="list-style-type: none"> 1. Ofimática 2. Fundamentos de redes 3. Dispositivos y servicios de red 4. Herramientas de redes y seguridad informática 5. Conocimiento Software de gestión de recursos 6. Conocimientos de planificación y control de tiempos 7. Conocimiento de gestión de cambios relacionado al modelo ITIL 	
CAMPO DE APLICACIÓN	
CATEGORIA:	CLASE:
1. Método	1.1. Manual 1.2. Automatizada
2. Ambiente:	2.1. Centro de cómputo 2.2. Oficina 2.3. Laboratorio piloto
3. Equipos y herramientas:	3.1. Computadoras 3.2. Ping/tracert 3.3. Generador de tráfico 3.4. Herramientas de captura/análisis de tráfico 3.5. Herramientas de gestión de proyectos

UNIDAD DE COMPETENCIA N° 02

Programador de servicios e infraestructura de redes y sistemas de seguridad informática.

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMÁTICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-002-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	2. Implementar servicios e infraestructura de redes y sistemas de seguridad informática de acuerdo al diseño y especificaciones técnicas según el plan operativo de la organización.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-002-RSI-V1-2016-EC01
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	2.1. Ejecutar el plan de seguridad de la información en la infraestructura de redes y seguridad informática de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
<p>ES COMPETENTE SI:</p> <p>A. La plantilla de línea base para los activos de la infraestructura de red y seguridad informática es elaborada de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.</p> <p>B. Las políticas de seguridad al plan de trabajo y seguridad informática son implementadas de acuerdo a los lineamientos estratégicos de la empresa y a los estándares vigentes.</p>	<p>DESEMPEÑO: Profesional Técnico ejecutando el plan de seguridad de la información en la infraestructura de red de seguridad informática.</p> <p>A. Elabora plantilla de línea base (condiciones mínimas o básicas) para los activos de la infraestructura de red de seguridad informática.</p> <ul style="list-style-type: none"> - Identifica los componentes de la política de seguridad de la información a aplicar. - Determina los parámetros de configuración de los equipos informáticos. - Implementa la plantilla de línea base (condiciones mínimas) en los distintos activos informáticos. <p>B. Implementa las políticas de seguridad al plan de trabajo y seguridad informática.</p> <ul style="list-style-type: none"> - Actualiza el plan de trabajo y documento de continuidad de servicio. - Determina las herramientas de seguridad de la información. - Determina las reglas a implementar en cada una de las herramientas de redes y seguridad. - Verifica el cumplimiento de la política de seguridad. <p>PRODUCTO:</p> <ul style="list-style-type: none"> - Plantilla de configuración de línea base (condiciones mínimas o básicas). - Plan de trabajo actualizado - Informe de implementación de la línea base (condiciones mínimas) <p>ACTITUDES: Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.</p>
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
<ol style="list-style-type: none"> 1. Ofimática 2. Sistemas operativos 3. Aplicativos de seguridad 4. Herramientas de seguridad y redes 5. Conocimientos de estándares y buenas prácticas 	
CAMPO DE APLICACIÓN	
CATEGORÍA:	CLASE:
<ol style="list-style-type: none"> 1. Método 2. Ambiente: 3. Equipos y herramientas: 	<ol style="list-style-type: none"> 1.1. Manual 1.2. Automatizada 2.1. Centro de computo 2.2. Oficina 2.3. Laboratorio piloto 3.1. Capturador de tráfico 3.2. Herramientas de análisis de vulnerabilidades y amenazas. 3.3. Herramienta de inventario de activos

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMATICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-002-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	2 Implementar servicios e infraestructura de redes y sistemas de seguridad informática de acuerdo al diseño, especificaciones técnicas y normas técnicas según el plan operativo de la organización.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-002-RSI-V1-2016-EC02
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	2.2 Instalar dispositivos y servicios de red y seguridad informática, de acuerdo normas técnicas vigentes.
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
ES COMPETENTE SI: <ul style="list-style-type: none"> A. El diagrama de topología de red es elaborada de acuerdo a normas técnicas vigentes. B. Los dispositivos y terminales son instalados según normas técnicas vigentes. C. Los dispositivos intermediarios son instalados según normas técnicas vigentes. D. Los servicios de red son instalados según normas técnicas vigentes. 	DESEMPEÑO: Profesional Técnico instalando dispositivos y servicios de red y seguridad informática. <ul style="list-style-type: none"> A. Elabora diagrama de topología de red <ul style="list-style-type: none"> - Realiza cálculos para dimensionar el requerimiento de insumos para el sistema de cableado estructurado. - Instala infraestructura física de red - Realiza chequeo del equipamiento utilizado en la red de acuerdo a las especificaciones de la topología sugerida. - Elabora diagrama de topología física y lógica - Identifica la función de los componentes de red. - Identifica la relación de los diferentes componentes de la red de datos. - Ubica los dispositivos de seguridad requeridos B. Instala dispositivos y terminales <ul style="list-style-type: none"> - Verifica especificaciones técnicas del producto. - Instala software y aplicaciones de escritorio y servidores. - Instala otros dispositivos de red C. Instala los dispositivos intermedios <ul style="list-style-type: none"> a. Instala dispositivos intermedios de conmutación b. Instala dispositivos intermedios de enrutamiento c. Instala dispositivos intermedios de seguridad. D. Instala servicios de red: <ul style="list-style-type: none"> a. Despliega servicios de red b. Despliega servicios de seguridad c. Implementa controles de seguridad PRODUCTO: <ul style="list-style-type: none"> - Informe de especificaciones. - Equipos y servicios instalados. - Manual de instalación de equipos y servicios. - Diagrama de topología de red ACTITUDES: <p>Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.</p>
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
<ol style="list-style-type: none"> 1. Hardware y software de computadoras. 2. Sistemas operativos. 3. Seguridad informática. 4. Ofimática 5. Fundamentos de red 6. Conocimientos básicos de electricidad 7. Conocimientos de cableado estructurado 8. Conocimientos de data networking 9. Proceso de gestión de configuración de ITIL 10. Proceso de cambios de ITIL 11. Proceso de validación y pruebas de servicio ITIL 	
CAMPO DE APLICACIÓN	
CATEGORIA:	CLASE:
1. Método	1.1 Manual
	1.2. Automatizada
2. Ambiente:	2.1. Centro de cómputo

3. Equipos y herramientas:

- 2.2.Oficina
- 2.3. Laboratorio piloto
- 3.1. Computadoras.
- 3.2. Protocolos de conexión remota
- 3.3. Herramienta de clonación

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMÁTICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-002-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	2 Implementar servicios e infraestructura de redes y sistemas de seguridad informática de acuerdo al diseño y especificaciones técnicas según el plan operativo de la organización.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-002-RSI-VI-2016-EC03
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	2.3. Configurar dispositivos y servicios de red y seguridad informática de acuerdo a normas vigentes.
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
ES COMPETENTE SI: A. Los dispositivos y servicios de red y seguridad informática son configurados de acuerdo a normas vigentes. B. La prueba de funcionamiento es realizada en equipos pilotos de acuerdo al tiempo establecido en el plan de implementación.	DESEMPEÑO: Profesional Técnico configurando dispositivos y servicios de red y seguridad informática. A. Configura dispositivos y servicios de red - Configura equipo de seguridad. - Configura dispositivos intermedios y terminales. - Mantiene documentación del estado de la red. B. Realiza prueba de funcionamiento - Verifica funcionamiento en un equipo según el perfil del usuario. - Genera errores y ataques de seguridad para comprobar funcionamiento del servicio. - Corrige y/o ratifica el servicio instalado. PRODUCTO: - Equipos y dispositivos configurados. - Reporte de estado de los equipos. - Reporte de pruebas - Informe de despliegue de servicios y controles de seguridad. ACTITUDES: Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
1. Hardware y software de computadoras. 2. Sistemas operativos. 3. Seguridad informática. 4. Redes 5. Conocimientos de data networking 6. Proceso de gestión de configuración de ITIL 7. Proceso de cambios de ITIL 8. Proceso de validación y pruebas de servicio ITIL	
CAMPO DE APLICACIÓN	
CATEGORÍA: 1. Método 2. Ambiente: 3. Equipos y herramientas:	CLASE: 1.1.Manual 1.2.Automatizada 2.1.Centro de cómputo/Oficina 2.2.Laboratorio piloto 3.1.Computadoras 3.2. Protocolo de descubrimiento de Vecinos

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMÁTICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-002-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	2 Implementar servicios e infraestructura de redes y sistemas de seguridad informática de acuerdo al diseño y especificaciones técnicas según el plan operativo de la organización.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-002-RSI-V1-2016-EC04
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	2.4 Verificar la operatividad de los dispositivos y servicios instalados de acuerdo al plan de implementación.
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
ES COMPETENTE SI:	DESEMPEÑO: El profesional técnico verificando la operatividad de los dispositivos y servicios instalados.
A. Las pruebas funcionales sobre equipos y servicios son ejecutados de acuerdo al plan de implementación.	A. Ejecuta pruebas funcionales sobre equipos y servicios <ul style="list-style-type: none"> - Selecciona los equipo de prueba - Verifica la instalación eléctrica de los dispositivos - Verifica la instalación de cableado de red - Valida la configuración de los equipos y redes instalados - Valida la configuración y el funcionamiento de los servicios configurados. - Realiza prueba piloto en los equipos de prueba - Realiza prueba de funcionalidad de equipos y servicios - Aplica pruebas de conectividad - Aplica pruebas de servicio
B. Las pruebas de estrés sobre equipos y servicios son aplicados de acuerdo al plan de implementación.	B. Aplica pruebas de estrés sobre equipos y servicios <ul style="list-style-type: none"> - Aplica generadores de tráfico en enlaces críticos - Realiza medición de ancho de banda en la red - Aplica carga sobre procesos y servicios. - Aplica criterios y pruebas de balanceo de tráfico - Genera errores para ver la respuesta en los equipos y servicios
C. Los procedimientos y herramientas para verificar nivel de seguridad de la red son aplicados de acuerdo al plan de implementación.	C. Aplica procedimientos y herramientas para verificar el nivel de seguridad de la red. <ul style="list-style-type: none"> - Aplica técnicas de penetración y seguridad a la red - Realiza pruebas de caja blanca y caja negra en la red - Aplica técnicas forenses de análisis (post mortem) de la seguridad de la red. - Realiza correcciones a las vulnerabilidades encontradas - Realiza monitoreo de incidentes en la red.
	PRODUCTO: <ul style="list-style-type: none"> - Informe de la prueba funcional. - Reporte de pruebas de red - Informe de nivel de seguridad. - Reporte de análisis forense - Reporte de configuración de los equipos - Reporte de las correcciones realizadas
	ACTITUDES: Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
<ol style="list-style-type: none"> 1. Hardware y software de computadoras. 2. Sistemas operativos. 3. Seguridad informática. 4. Redes y conectividad 5. Hackeo ético (ética hacking) 6. Conocimientos de electricidad básica 7. Conocimientos de data networking 8. Proceso de validación y pruebas de servicio ITIL 	
CAMPO DE APLICACIÓN	
CATEGORIA:	CLASE:
1. Método	1.1.Manual 1.2.Automatizada

2. Ambiente:	2.1.Centro de cómputo/ Oficina
3. Equipos y herramientas:	2.2.Laboratorio piloto
	3.1.Computadoras
	3.2.Técnicas de hacking
	3.3. Herramientas de análisis forense
	3.4. Herramientas de gestión o administración de red

UNIDAD DE COMPETENCIA N° 03

Mantenimiento de la funcionalidad y seguridad de los servicios de redes y servicios de seguridad informática

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMÁTICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-003-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	3 Mantener la funcionalidad y seguridad de los servicios de redes y servicios de seguridad informática, de acuerdo a los lineamientos establecidos por la organización.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-003-RSI-V1-2016-EC01
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	3.1. Monitorear el funcionamiento de la infraestructura de redes y seguridad informática de acuerdo a los lineamientos establecidos por la organización
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
<p>ES COMPETENTE SI:</p> <p>A. El funcionamiento de la infraestructura de redes es verificado de acuerdo a los lineamientos establecidos por la organización.</p> <p>B. Los servicios de redes implementados en la organización son monitoreados de acuerdo a los lineamientos establecidos por la organización.</p> <p>C. El estado del sistema de seguridad informática es verificado de acuerdo a los lineamientos establecidos por la organización</p>	<p>DESEMPEÑO: Profesional Técnico monitoreando el funcionamiento de la infraestructura de redes y seguridad informática.</p> <p>A. Verifica funcionamiento de la infraestructura de redes</p> <ul style="list-style-type: none"> - Realiza operaciones físicas con el equipamiento. - Accede a la configuración de los equipos - Realiza pruebas de funcionamiento de equipos <p>B. Monitorea los servicios de redes implementados en la organización</p> <ul style="list-style-type: none"> - Verifica la configuración de los servicios de redes - Mide parámetros de desempeño de los servicios de redes - Captura tráfico de red <p>C. Verifica el estado del sistema de seguridad informática</p> <ul style="list-style-type: none"> - Realiza pruebas de seguridad informática - Revisa configuración de las herramientas de seguridad informática. - Revisa la configuración de reglas de seguridad - Revisa los archivos de información de logs - Analiza el tráfico de red <p>PRODUCTO:</p> <ul style="list-style-type: none"> - Check list del status del equipamientos - Reporte de configuración de los equipos - Reporte de status de los servicios de redes - Registro de incidentes - Reporte de status de los sistemas de seguridad <p>ACTITUDES:</p> <p>Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.</p>
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
<ol style="list-style-type: none"> 1. Manejo de configuración de equipos de redes 2. Procedimientos de diagnóstico de hardware 3. Software de diagnóstico de redes 4. Herramientas de gestión de servicios 5. Protocolo de comunicaciones 6. Manejo de software de auditoria de redes 7. Conocimiento de administración de redes 8. Proceso de gestión de incidentes del ITIL 	
CAMPO DE APLICACIÓN	
CATEGORIA:	CLASE:
4. Método	1.1 Manual 1.2 Automatizada 2.1 Oficina local 2.2 Oficina remota
5. Ambiente:	3.1 herramientas de testeo de los servicios de redes 3.2 sensores de red (IPS, IDS)
6. Equipos y herramientas:	3.3 sensores de temperatura y de humedad

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMÁTICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-003-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	3 Mantener la operatividad y seguridad de los servicios de redes y seguridad informática, de acuerdo a los lineamientos establecidos por la organización.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-003-RSI-V1-2016-EC02
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	3.2 Diagnosticar el estado de los dispositivos y servicios de redes de acuerdo a los lineamientos establecidos por la organización.
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
ES COMPETENTE SI: A. Los dispositivos de la estructura de redes y servicios es revisado de acuerdo a los lineamientos establecidos por la organización. B. Los resultados del examen realizado es analizado de acuerdo a los lineamientos establecidos por la organización.	DESEMPEÑO: Profesional técnico diagnosticando el estado de los dispositivos y servicios de redes. A. Revisa los dispositivos de la estructura de redes y servicios - Equipo de enrutamiento - Equipo de enlace - Servicios de internet B. Analiza los resultados del examen realizado - Compara los resultados con los lineamientos establecidos. - Determina el estado de los dispositivos. PRODUCTO: - Reporte de equipos con configuraciones - Reporte de valores mínimos y máximos - Reporte de diagnóstico del estado de los dispositivos y servicios de redes. ACTITUDES: Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
1. Protocolo de redes y comunicaciones 2. Normas técnicas relacionadas (IEEE) 3. Manejo de equipos electrónicos y eléctricos 4. Conocimiento de equipo de comunicaciones.	
CAMPO DE APLICACIÓN	
CATEGORIA: 1. Método 2. Ambiente: 3. Equipos y herramientas:	CLASE: 1.1.Manual 1.2.Automatizada 2.1. Centro de computo 2.2. Oficina de servicios de redes 3.1. Software de captura y análisis de tráfico de red.

DENOMINACIÓN DE LA PROFESIÓN TÉCNICA	REDES Y SEGURIDAD INFORMÁTICA
CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-003-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	3. Mantener la funcionalidad y seguridad de los servicios de redes y seguridad informática, de acuerdo a los lineamientos establecidos por la organización.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-003-RSI-VI-2016-EC03
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	3.3.Ejecutar el plan de mantenimiento preventivo y correctivo de la infraestructura de redes, seguridad y servicios de acuerdo a las políticas de la organización y normas vigentes
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
<p>ES COMPETENTE SI:</p> <p>A. El mantenimiento preventivo del hardware y software de redes y seguridad informática es planificado de acuerdo a las políticas de la organización y normas vigentes.</p> <p>B. El plan de mantenimiento preventivo es ejecutado de acuerdo a las políticas de la organización y normas vigentes.</p> <p>C. Las vulnerabilidades en el hardware y software de redes y seguridad informática son detectadas de acuerdo a las políticas de la organización y normas vigentes.</p>	<p>DESEMPEÑO: Profesional técnico ejecutando el plan de mantenimiento preventivo de la infraestructura de redes, seguridad y servicios.</p> <p>A. Planifica el mantenimiento preventivo y correctivo de hardware y software de redes y seguridad informática:</p> <ul style="list-style-type: none"> - Elabora el cronograma de mantenimiento preventivo - Realiza reemplazo de hardware y software de redes y seguridad de los equipos - Programa las actualizaciones de firmas antivirus y sistemas operativos <p>B. Ejecuta el plan de mantenimiento preventivo y correctivo</p> <ul style="list-style-type: none"> - Comprueba el estado del hardware y software de redes y seguridad informática - Documenta las tareas de mantenimiento aplicadas en hardware y software. - Realiza mantenimiento de hardware de primer y segundo nivel. - Ejecuta el mantenimiento correctivo del hardware y software de redes y seguridad informática - Ejecuta actualización de firmware. <p>C. Detecta vulnerabilidades en el hardware y software</p> <ul style="list-style-type: none"> - Aplica herramientas de optimización de software para sistemas operativos de usuario final y servidores. - Ejecuta análisis de seguridad contra malware - Reporta amenazas el día 0. - Comprueba vulnerabilidades en el hardware y software - Establece correcciones a las vulnerabilidades encontradas en el hardware y software. <p>PRODUCTO:</p> <ul style="list-style-type: none"> - Informe de mantenimiento preventivo del software y hardware de redes y seguridad informática. - Informe de actualización del hardware y software de redes y seguridad informática. - Informe del estado del hardware y software de redes y seguridad informática. - Informe de vulnerabilidades de redes y seguridad informática

	<p>- Informe de mantenimiento correctivo</p> <p>-</p> <p>ACTITUDES: Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.</p>
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
<ol style="list-style-type: none"> 1. Normas técnicas 2. Estándares de seguridad 3. Estándares de redes 4. Vulnerabilidades en hardware y software de redes y seguridad informática. 5. Estándares en gestión de servicios informáticos (ITIL) 6. Estándares de garantía de equipos 7. Conocimientos básicos de electrónica 	
CAMPO DE APLICACIÓN	
<p>CATEGORIA:</p> <ol style="list-style-type: none"> 1. Método 2. Ambiente: 3. Equipos y herramientas: 	<p>CLASE:</p> <ol style="list-style-type: none"> 1.1. Manual 1.2. Automatizada 2.1. Centro de cómputo/Oficina 2.2. Computadoras 3.2. Software de gestión de actualización de antivirus 3.3. Software de gestión de actualización de sistemas operativos.

CÓDIGO DE LA NORMA DE COMPETENCIA	NCPT-003-RSI-VI-2016
DENOMINACIÓN DE LA NORMA DE COMPETENCIA	3 Mantener la operatividad y seguridad de los servicios de redes y seguridad informática, de acuerdo a los lineamientos establecidos por la organización.
CÓDIGO DEL COMPONENTE NORMATIVO	NCPT-003-RSI-V1-2016-EC04
DENOMINACIÓN DEL ELEMENTO DE COMPETENCIA	3.4. Ejecutar el plan de respuesta a incidentes de redes y seguridad informática de acuerdo a los lineamientos establecidos por la organización
CRITERIOS DE DESEMPEÑO	EVIDENCIAS
ES COMPETENTE SI: A. Los incidentes de redes y seguridad informática son identificados de acuerdo a los lineamientos establecidos por la organización. B. Las acciones a ejecutar son determinadas de acuerdo a los lineamientos establecidos por la organización.	DESEMPEÑO: Profesional técnico ejecutando el plan de respuesta de incidentes de redes y seguridad informática. A. Identifica incidentes - Identifica los incidentes físicos y lógicos de redes - Identifica los incidentes físicos y lógicos de seguridad informática - Detecta vulnerabilidades de las redes y seguridad informática. B. Determina acciones a ejecutar - Establece las contramedidas a aplicar - Envía alertas a los administradores de red - Ejecuta las contramedidas PRODUCTO: - Lista de incidentes físicos y lógicos de redes - Lista de incidentes físicos y lógicos en seguridad informática - Reporte de solución de incidentes ACTITUDES: Trabajo en Equipo, ética, calidad y mejora continua, adaptabilidad a los cambios del entorno, toma de decisiones, tolerancia a la presión de trabajo, productividad, compromiso con la calidad de trabajo, credibilidad técnica y comunicación eficaz.
CONOCIMIENTOS FUNDAMENTALES (evidencias del saber):	
1. Conocimientos de tipos de vulnerabilidades y amenazas 2. Manejo de software para detectar vulnerabilidades y amenazas 3. Manejo de herramientas de software para resolver los problemas en redes de datos y seguridad informática. 4. Herramientas de captura y análisis de tráfico de red 5. Procedimientos para el diagnóstico de vulnerabilidades y amenazas 6. Conocimientos básicos de electrónica	
CAMPO DE APLICACIÓN	
CATEGORIA: 1. Método 2. Ambiente: 3. Equipos y herramientas:	CLASE: 1.1. Manual 1.2. Automatizado 2.1. Oficina 2.2. Centro de cómputo 3.1. Software de captura y análisis de tráfico de red 3.2. Software de análisis de vulnerabilidades y pruebas de penetración. 3.3. Sistema de correlación de eventos.