CCL | CÁMARA DE COMERCIO LIMA

Educación ejecutiva

+30 AÑOS CAPACITANDO

CURSO DE ESPECIALIZACIÓN

Administración de **Redes** e **Informática forense**

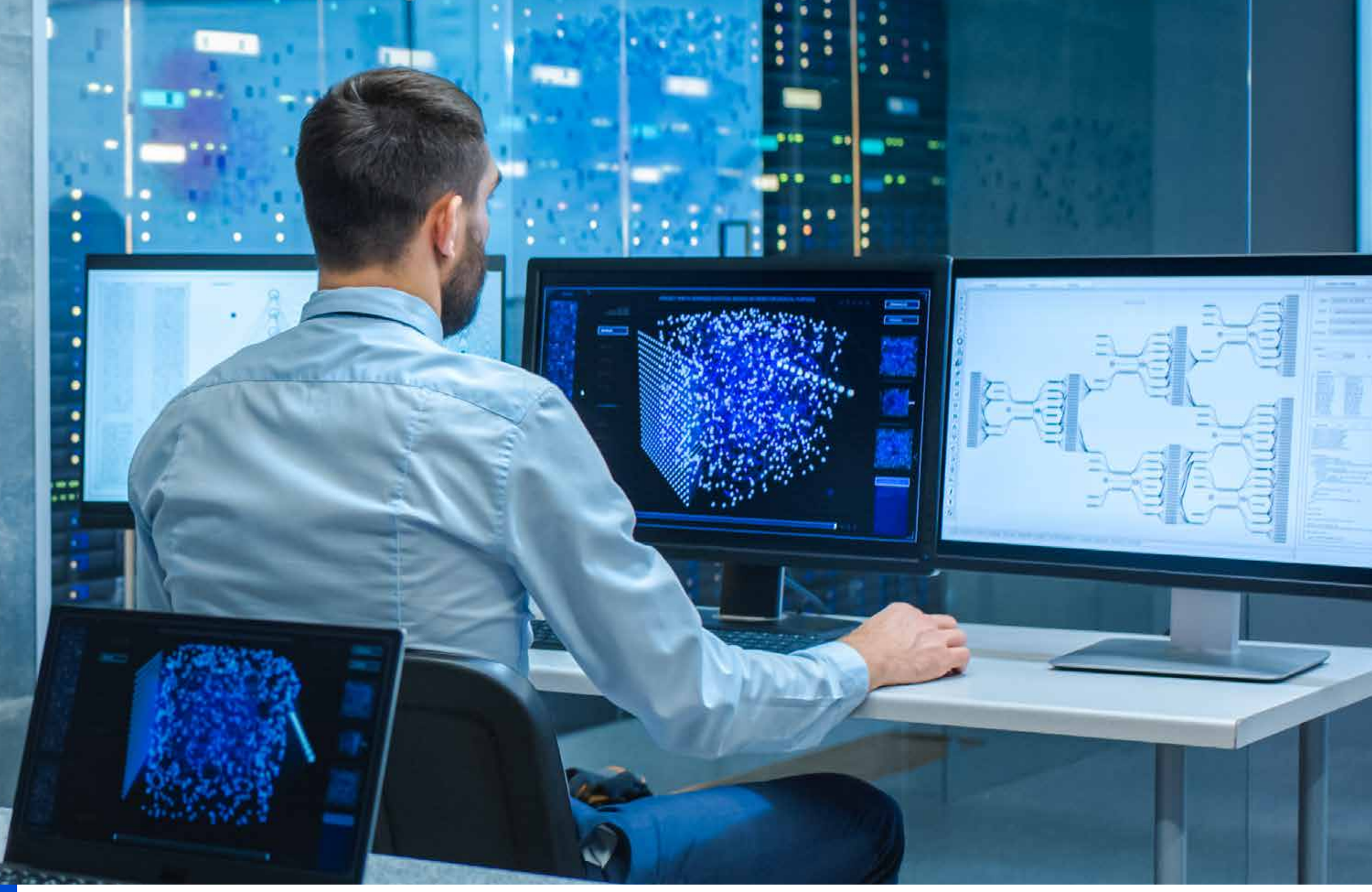
Certifica el Centro de Transformación Digital de la CCL

INTRODUCCIÓN

Con este curso aprenderás los principios básicos, así como las técnicas para detectar y responder a las amenazas de ciberseguridad. Aprenderás a manejar varios tipos de incidentes, las metodologías de evaluación de riesgos y las normativas relacionadas al manejo de incidentes. Al finalizar este curso, estarás en la capacidad de crear políticas de manejo de respuesta a incidentes de Ciberseguridad.

Comprenderás como aplicar las normativas ISO/IEC 27001 – ISO/IEC 27035 – ISO/IEC 27002. Además, conocerás las mejores prácticas para la prevención de actividades delictivas en internet, cibercrimen y fraude online. Estarás preparado para una gestión proactiva, que garantice la seguridad de la actividad digital en tu empresa u organización.

La Ciberseguridad se ha convertido en uno de los mayores retos que debemos afrontar hoy en cualquier organización. Es imperativo proteger al principal activo empresarial: la información, la que se comparte a través de diferentes dispositivos conectados a Internet. Una deficiente gestión de la Ciberseguridad puede tener un gran impacto económico en la empresa. Pero también el impacto es a nivel reputacional, puesto que afecta la confianza de socios estratégicos y clientes.



OBJETIVOS

- Adquirir habilidades técnicas para la administración de redes e informática forense.

- Identificar y responder a incidentes de ciberseguridad, siguiendo estándares y las mejores prácticas de la industria.

- Desarrollar experiencia práctica en técnicas de informática forense, para identificar, analizar y presentar evidencia digital en escenarios de investigación realistas.

DIRIGIDO A

- Profesionales de TI y Administradores de Red: Responsables de la gestión, mantenimiento y seguridad de las redes y sistemas informáticos en sus organizaciones.

- Responsables de Ciberseguridad y Respuesta a Incidentes: Profesionales encargados de la protección contra amenazas cibernéticas, así como la gestión de incidentes de ciberseguridad.

- Personal de Fuerzas de Seguridad y del Ministerio Público: Involucrados en investigaciones de delitos cibernéticos y forenses digitales. Profesionales que requieran adquirir o mejorar, sus habilidades técnicas en informática forense y gestión de incidentes.

TEMARIO

MÓDULO I: CONECTIVIDAD Y REDES IP

En este módulo, los participantes explorarán los fundamentos esenciales que permiten la comunicación y gestión efectiva dentro de las redes informáticas. Conocerán cómo están estructuradas las redes, cómo los dispositivos dentro de estas redes obtienen y utilizan las direcciones IP para comunicarse. Además, el cómo se pueden segmentar y administrar estas redes, para mejorar la seguridad y la eficiencia. Se abordarán en detalle aspectos como:

- **DHCP (Protocolo de Configuración Dinámica de Host):** Se explorará cómo configurar y administrar un servidor DHCP. Así mismo, el cómo garantizar la asignación correcta de direcciones IP para facilitar la comunicación en la red.

- **DNS (Sistema de Nombres de Dominio):** Se explorará el funcionamiento del sistema DNS, cómo traduce los nombres de dominio en direcciones IP. Además, de su importancia en la navegación web y la resolución de nombres en una red.

- **VLAN (Red de Área Local Virtual):** Se abordará la creación y gestión de VLANs para segmentar una red física en múltiples redes lógicas. También, el cómo las VLANs pueden mejorar la seguridad y eficiencia de la red.

- **Inter-VLAN Routing:** Se abordará el enrutamiento entre diferentes VLANs, permitiendo la comunicación entre dispositivos en diferentes segmentos de red. Se explorarán también, las configuraciones necesarias en dispositivos como los enrutadores o switches de capa 3, para facilitar el enrutamiento Inter-VLAN.

MÓDULO II: ADMINISTRACIÓN EN WINDOWS SERVER 2016

En este módulo los participantes profundizarán en la gestión y configuración de los servicios esenciales proporcionados por Windows Server 2016. Descubrirán cómo configurar, administrar y mantener servicios críticos de red y servidor en un entorno empresarial. Se profundizarán en aspectos como:

- **Directorio Activo (AD):** Se abordará el servicio de Directorio Activo, que es central para la gestión de identidades y políticas en una red empresarial. Se explorará cómo configurar y administrar un dominio, cómo gestionar usuarios y grupos, y cómo implementar políticas de grupo (GPOs). Los participantes lograrán entender cómo el AD contribuye a la seguridad y gestión eficiente de la red.

- **DNS (Sistema de Nombres de Dominio):** Se explorará la configuración y gestión del servicio DNS en Windows Server 2016. Se abordará cómo resolver nombres de dominio, configurar zonas de búsqueda directa e inversa. Así mismo, cómo el servicio DNS interactúa con el Directorio Activo para facilitar la resolución de nombres en la red empresarial.

- **Failover DHCP (Protocolo de Configuración Dinámica de Host con conmutación por error):** Se abordará la configuración y gestión de la alta disponibilidad para el servicio DHCP, utilizando la característica de Failover DHCP. Los participantes aprenderán cómo configurar un ambiente de failover DHCP, para garantizar la continuidad del servicio de asignación de direcciones IP, en caso de fallos del servidor.

- **IIS (Servicios de Información de Internet):** Se explorará la configuración y administración del servidor web IIS. Los participantes aprenderán cómo hospedar sitios web y aplicaciones, gestionar certificados SSL/TLS, configurar listas de control de acceso (ACLs) y entender cómo optimizar el rendimiento y la seguridad del servidor web.

MÓDULO III: CONFIGURACIÓN Y SOPORTE

En este módulo, los participantes descubrirán aspectos esenciales sobre la configuración, gestión, así como del soporte continuo de los servicios y recursos de red, en un entorno empresarial. Desarrollarán habilidades prácticas para la implementación y administración de políticas de grupo, gestión de recursos del servidor, y estrategias de backup. Aspectos que son críticos para mantener la integridad, seguridad y disponibilidad de los datos y servicios en una organización. Se abordarán en detalle aspectos como:

- **GPOs (Políticas de Grupo):** Las Políticas de Grupo (GPOs) son una característica central en la administración de entornos de Windows. Permite a los administradores configurar, así como aplicar configuraciones y políticas específicas en toda la organización. Se abordará el cómo crear, configurar y administrar GPOs. Así mismo, el cómo pueden ser utilizadas para mejorar la seguridad, configuración y gestión de las estaciones de trabajo y servidores.

- **File Server Resources Manager (FSRM):** FSRM es una herramienta que permite a los administradores gestionar y monitorizar los recursos del servidor de archivos. Se profundizará en el cómo configurar cuotas, filtros de archivos, y generar informes para monitorear el uso del espacio en disco. Además, se abordará cómo FSRM puede ayudar en la identificación y gestión de datos sensibles o regulados.

- **Backups:** Se abordarán las estrategias y soluciones de backup para garantizar la recuperación de datos en caso de fallos o incidentes de ciberseguridad. Se explorará sobre los diferentes tipos de backups, cómo planificar y configurar backups regulares, y cómo restaurar datos de los backups cuando sea necesario.

MÓDULO IV: GESTIÓN DE INCIDENTES Y PROCESO DE INVESTIGACIÓN DE UN ANÁLISIS FORENSE INFORMÁTICO

En este módulo, los participantes lograrán una comprensión profunda de las metodologías y estándares líderes en la industria, para gestionar incidentes de ciberseguridad y realizar análisis forenses informáticos. Se abordará el cómo responder eficazmente ante incidentes de ciberseguridad. Así mismo, el cómo investigar y analizar los incidentes de manera metódica, y conforme a las normativas vigentes.

Normativas y Estándares:

- **NIST (Instituto Nacional de Estándares y Tecnología):** Se explorarán las guías y Frameworks proporcionadas por el NIST, enfocados en la gestión de incidentes de ciberseguridad. Los participantes aprenderán, cómo estos frameworks pueden ayudar a las organizaciones a prepararse, responder y recuperarse de los incidentes de seguridad.

- **ISO 27035 (Gestión de incidentes de seguridad de la información):** Se abordará la norma ISO 27035, que proporciona un enfoque estructurado para la gestión de incidentes de ciberseguridad. Se explorará las fases del proceso de gestión de incidentes, y cómo implementar un proceso de respuesta a incidentes efectivo.

- **ISO 27001 (Sistemas de gestión de seguridad de la información) y ISO 27002 (Código de práctica para controles de seguridad de la información):** Se abordarán estas normas internacionales, que proporcionan los requisitos y mejores prácticas para la gestión de la seguridad de la información.

- **SBS 504 (Gestión de incidentes en servicios financieros):** Se explorará la guía SBS 504, y cómo se aplica a la gestión de incidentes en el sector financiero.

Proceso de Investigación de un Análisis Forense Informático

Se explorará los pasos y técnicas involucradas en la realización de un análisis forense informático. Se cubrirá, desde la identificación y preservación de evidencia digital, hasta el análisis y presentación de los hallazgos forenses. Los participantes aprenderán cómo llevar a cabo investigaciones forenses de manera ética y efectiva. Y, asegurando la integridad de la evidencia, así como la adhesión a los procedimientos legales y normativos.

MÓDULO V: INFORMÁTICA FORENSE EN SISTEMAS OPERATIVOS (WINDOWS Y LINUX)

En este módulo los participantes desarrollarán conocimientos y habilidades prácticas, para realizar investigaciones forenses en los entornos de sistemas operativos predominantes. La informática forense es esencial para investigar incidentes de ciberseguridad, fraudes, mal uso de datos y otros delitos cibernéticos. Proporciona evidencia digital, que puede ser utilizada en procedimientos legales. Se abordarán las técnicas y herramientas utilizadas en la extracción, análisis y presentación de evidencia digital en sistemas operativos Windows y Linux.

- **Informática Forense en Windows:** Se explorarán las técnicas y herramientas específicas utilizadas para llevar a cabo investigaciones forenses en entornos Windows:
    - Extracción y análisis de registros del sistema y del registro de Windows.
    - Identificación y recuperación de datos borrados.
    - Análisis de artefactos del sistema, como archivos prefetch, puntos de restauración del sistema y archivos de paginación.
    - Utilización de herramientas forenses específicas para Windows.

- **Informática Forense en Linux:** Se abordarán las técnicas y herramientas específicas para la informática forense en entornos Linux:

- Extracción y análisis de logs del sistema y otros artefactos forenses.
- Identificación y recuperación de datos borrados.
- Análisis de la línea de tiempo del sistema y artefactos de memoria.
- Utilización de herramientas forenses específicas para Linux.

MÓDULO VI: LABORATORIO DE CASOS

En este módulo los participantes aplicarán los conocimientos adquiridos en el curso, en un entorno práctico y controlado. Con ejercicios de laboratorio basados en casos reales, trabajarán en escenarios prácticos de análisis forense y gestión de incidentes. Obtendrán una experiencia práctica intensiva, que les permitirá resolver desafíos realistas, bajo la guía de un instructor altamente especializado. Se profundizarán en aspectos como:

- **Revisión de Logs:** Los participantes aprenderán cómo revisar y analizar logs de sistemas y aplicaciones para identificar actividades sospechosas o malintencionadas. Se abordarán técnicas para filtrar, correlacionar y interpretar datos de logs.

- **Dump de Memoria RAM:** Los participantes aprenderán cómo realizar un dump (volcado) de la memoria RAM de un sistema. Así mismo, cómo analizar estos dumps para extraer información valiosa, que puede ser utilizada en la investigación forense.

- **Recuperación de Archivos en Linux:** Los participantes aprenderán técnicas y herramientas, para recuperar archivos borrados o corruptos en sistemas operativos Linux. También se explorarán métodos para analizar sistemas de archivos y recuperar datos.

- **Generación de Hash:** Los participantes aprenderán la importancia de las funciones hash en la informática forense. Se enseñará cómo generar valores hash para validar la integridad de los datos. Así mismo, cómo utilizar los hashes para verificar la autenticidad de la evidencia digital.

EXPOSITOR

Mg. Ing. CIP Luis Gastulo Salazar

Sub Gerente de Seguridad Ofensiva en MiBanco

Ingeniero de Sistemas y cómputo de la Universidad Inca Garcilaso de la Vega, con grado de Magister en Ingeniería de Seguridad Informática de la Universidad Tecnológica del Perú. Así mismo, tiene el grado de Magister en Dirección de Tecnologías de información de la Universidad ESAN.

Se ha desempeñado anteriormente como, Jefe de Ciberseguridad, Aplicación y Datos en Banco Ripley Perú. Así mismo, como Jefe de Seguridad de la Información en el Ministerio de Educación.

DURACIÓN:

6 semanas

MODALIDAD:

100% virtual

INVERSIÓN:

Tarifa regular: S/ 720
Socio CCL: S/ 540

CERTIFICA:

Centro de Transformación Digital de la Cámara de Comercio de Lima

MÉTODOS DE PAGO

- **Depósitos o transferencia** Cuenta corriente en soles banco

Banco o agente BCP
193-1943271-0-99

Banco o agente Interbank
005-0000007180

Banco BBVA
0011-0130-0100003020

Banco Scotiabank
000-2019361

Todas nuestras cuentas están a nombre de **CÁMARA DE COMERCIO DE LIMA – Ruc:** 20101266819

- **Tarjeta de crédito** Podrá realizar sus pagos con rapidez y total seguridad.

1. Ingresar a nuestra página web: **www.camaralima.org.pe**
2. Buscar: **Pagos online,** parte superior derecha.
3. Ingresar **datos de la empresa y/o persona** que solicito el servicio.
4. Ingresar **datos de la tarjeta de crédito y detalle del servicio.**
5. Procesar pago.

   Luego de realizar el pago, enviar el voucher de pago indicando el RUC y/o DNI del depositante al **asesor educativo.**

Hasta 3 cuotas sin intereses* con tus tarjetas de crédito
(*)Preguntar por términos y condiciones

- **Billetera electrónica** Escanea y paga

Considerar

Los horarios que están en la programación de todos los eventos que se realice están sometidos a cualquier cambio por cualquier inconveniente que se presente. ***Los cambios de los horarios serán notificados con anticipación.**

CCL | CÁMARA DE COMERCIO LIMA

CONTÁCTANOS

knunez@camaralima.org.pe

955 226 744