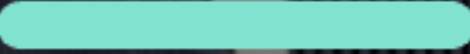




Being Safe or Feeling Safe?



Our team

Golden Projects LLC is an American company formed by experienced ICT consultants.

It provides cybersecurity and IT ecosystem management services to small and medium-sized enterprises.

Our experience is synonymous with infrastructure improvement and reliability, we identify risks, vulnerabilities and ensure continuity and efficiency through continuous innovation.

Our mission



Founded in 2016, Golden Projects LLC is the result of twenty years of experience targeting a multi-sector international market.

Our portfolio includes partnerships with Airports, Football Leagues, Nautical Companies, Banks and Entertainment Broadcasting Video Companies.

The goal is to design a secure and performing network that ensures the achievement of positive business results, using the best software and hardware tools available.



ICT
Consulting



Network
systems
management



Business
continuity
security



Cloud services



Cybersecurity



Pentesting

Our services



DDOS L4/L7
Protection



Hosting
Strategy



Training



Disaster
Recovery
Plan



Video
Broadcasting



Email service
management



ICT Consulting

- We meet customers and define the objective of the ICT consultancy together, facilitating the dialogue between infrastructure and software.
- We analyse the characteristics and specifications of corporate IT systems
- We propose solution packages suitable for different levels of complexity, to give value to the business and meet corporate needs
- We implement new software, hardware, network systems to improve the work experience
- We collaborate with the customer in order to make the best use of web tools in complete security
- We optimise business flows and daily routines
- We administer Windows, Mac OSX, Linux/Unix, iOS/Android platforms



Network systems management

Having a complete view of infrastructure vulnerabilities helps to optimise breakpoints and increase work performance.

Strategies are then suggested for the following points:

- Maintaining network efficiency
- Managing connectivity and interconnections between sites (VPN)
- Internet and intranet traffic filtering and analysis
- Implementation of customised services designed to facilitate the corporate goal

A fundamental aspect for the success of the business is to guarantee its continuity, through a number of key points:

- Balancing internet traffic across multiple providers
- Securing the company perimeter after analysing and filtering network traffic with a suitable firewall
- Creation of customised VPNs for secure remote access
- Virtualisation of workstations to improve security of Windows, Linux, Ultra-thin client



Business continuity security

The first choice for storing company data is cloud services.


Data is sent to online platforms that ensure it is available and can be retrieved at any time.

Cloud services are important for:

- Efficiency.
- Accessibility from any device connected to the Internet
- Avoiding data loss due to hardware malfunctions of storage devices within the company

The second choice of data storage is based on local datastores in the internal network (NAS) in order to:

- Store sensitive data without exposing them to the web
- Allow consultation only from within the company network
- Guarantee their deletion without leaving a trace.



Cloud services

One of the most neglected factors by companies is certainly computer security.

In the modern age, and especially in this particular period of history, we are increasingly witnessing data leaks aimed at accessing, transforming or destroying sensitive information, as well as extorting money from users or disrupting normal business processes.

Cybersecurity is the practice of protecting systems, networks and programmes from digital attacks.

Our company's main objective is

- Protect sensitive customer data
- Secure websites and online services at the perimeter
- Securely authenticate remote interfaces
- Provide access to company files via VPN
- Analysing network devices to minimise the risk of exposure to ransomware and Trojans
- Raise customer awareness of the correct use of the tools provided



Cybersecurity



Pentesting

Pentesting is carried out on online services, websites, Wifi access, VPN access, public shared folders and intranets.

- We carry out simulations of cyber attacks through third-party systems using the most advanced technologies
- We analyse the most significant vulnerabilities in real time and then introduce systems that can monitor any attacks or anomalies, blocking a certain type of outgoing or incoming traffic



DDOS L4/L7 Protection

Exposing your website or service online carries exponential risks every day.

Cyber attacks are very often carried out to

- Obtain company information
- Impact the operation of services
- Extort information from third-party customers and ask for money in return
- Obtain information for resale on the dark web
- Delete data and disrupt business continuity

By applying the right front-end technologies to exposed online services, DDoS attacks can be avoided at peak usage times.

Securing the back-end from unauthorised access ensures business continuity.

A good hosting strategy, coupled with good security, ensures the continuous provision of online and web services based on:

- Data duplication on multiple servers (balancing)
- Geolocalisation of traffic based on the user's current location (CDN)
- Continuous operation in case of failed PoPs (points of presence) (failover)



Hosting Strategy

Customised corporate training courses:

- Acquisition of the necessary skills for the independent handling of simple issues
- Prevention from backdoors (ransomware and Trojans)
- Secure attachment management
- Secure browsing modes
- Password security according to criteria
- Education in good daily habits for safeguarding company data



Training

The Disaster Recovery Plan is a digital strategy for dealing in the best possible way with an unforeseen event of any kind (malfunction, destruction, corruption, tampering by hackers, natural disasters, etc.) through some important regulations:

- Data backup outside the data centre or cloud
- Fire door in the data centre room
- Daily maintenance of total and incremental backups

Why your company should have a DRP:

- To limit economic damage from an unforeseen incident
- To limit damage to your image or customers from an unforeseen incident
- To limit digital service interruptions and/or disruption
- To prepare your staff to better manage emergencies
- To have a quick and effective emergency recovery plan ready at all times



Disaster Recovery
Plan

Due to the use of geolocalised servers (CDN), we are able to provide a customised video hosting/streaming service for

- Corporate events
- Trade fairs
- Conferences
- Videoconferences



Video Broadcasting

Today's market offers numerous solutions for the management of email services.

Our company is able to

- Analyse and identify the needs of each customer and suggest the best strategy to guarantee the confidentiality of sensitive data
- Manage customised whitelists/blacklists and newsletters through private servers
- Ensure daily backups of the company's email flow



Email service management

2022 economic forecast of global cybercrime damage

\$6
trillion

per year

\$16
billion

per day

\$500
billion

per month

\$115
billion

per week

\$684
million

per hour

\$11
million

per minute

\$190,000

per hour



Cybersecurity statistics for 2022



85%

of all cyber security breaches are caused by human error

94%

of all malware is delivered by email

10
seconds

is the frequency in which ransomware attacks occur

71%

of all cyber attacks are financially motivated (followed by intellectual property theft and then espionage)

10,5
trillion

is the estimated annual global cost of cybercrime

Security. Strategy. Reliability.

 **Golden Projects LLC**



WWW

golden-projects.com



goldenprojectsllc@gmail.com