Issue number 1. 2024

IMPACTO

by OCP TECH

DOSSIER
Smart Cities

PANEL DISCUSSION
Human Beings and their voice to enhance customer experience

PAIRS
Fraud and Cybersecurity

Digital edition

OCP TECH

IMPACT ENGINEERING

Of accelerations and reunions

The world of technology and the corporate landscape have interconnected us at an accelerated pace for some time now. The expansive nature of technology feeds back into its own growth and speed.

And here we are, navigating a world that, despite the challenges posed by a pandemic and physical distancing, has managed to resist a global crisis through ICT developments, reshaping aspects of our social, economic, and cultural dynamics. These changes will likely become clearer in the coming years.

We know that new developments find us with an increasingly larger infrastructure to work with, intensifying our efforts and diversifying our tasks even further. Between "to-dos" and aspirations, we might experience a sense of vertigo. Therefore, I invite us to establish connections and reflect on what is important, what is urgent, and what is necessary.

IMPACTO by OCP TECH emerges as a response to the need to pause, look around, broaden our vision, and gain perspective. We live in a technology-integrated ecosystem that must necessarily loop back to people. The only way to offer solutions and create impact is by expanding without losing focus on our humanity, being aware of the social impact that we can create. Understanding that, this magazine transforms into a resource for everyone—from students to executives—seeking to flip the switch on reset and make use of a space for reading and questioning to reunite somehow along the way.

Flor Palazzolo
Strategic Communications Director

OCP TECH Latin America

Founder and CEO
Leonardo Scatturice

COO
Andrés Quinn

CFO
Fernando Antolín Dulac

Regional Sales Director NOLA & Caribbean
Cesar Calderón

VP Sales NOLA
Hernán Piñero

VP Sales SOLA
Jorge Pinjosovsky

CLO
Josefina Eizayaga

Compliance Officer
Lucio Primucci

CIO
Ariel Castaño

CDO
Mauro Nunes

CX Regional Manager
Nadia Simón

HR Manager
Verónica Funes

Strategic Communications Director
Flor Palazzolo

SUMMARY

CX Files

by **Pablo Marrone**
CX and Communication Advisor

User **experience** is one of the key success factors in an organization. In this article, you will learn which are the main points that should be considered when developing a strategy focused on customer **satisfaction.**

everything Everywhere All at Once

The title of the Oscar-winning movie summarizes what should be expected from the Customer Success or Customer Experience areas. Reality shows us that we are far from that. Let's see some examples.

These are times of acceleration in terms of implementing CX/CS practices in organizations around the world. The topic is included on the agenda of all meetings and the most common questions that arise are similar among leaders: How can we do it? Where can we find good CSMs (Customer Success Managers)? What kind of tool should we use: a proprietary or a purchased software? How much of our recurring revenue should we invest in it? How can we improve the renewal rate?, among others.

Doubts are also common: Is it really worth it? Is it useful for medium-sized organizations? Do customers find it relevant?, just to name a few. Ultimately, there are 2 key questions that are usually not asked or that remain unanswered.

1.- What is the business model of the CX/CS area?

Without a business model, there is no valid CX practice, and thus several aspects are affected, including the contribution to cash flows, the necessary investment, the key accounts, the necessary team and its interaction with all areas, the impact on the rest of the roles, and both internal and external communication.
One of the most common mistakes is to assume that CX is an extension of another area. This mistake becomes even worse when it is included in Sales, as it clouds its benefits and ends up distorting its purpose in most cases. The results are not so bad when it is included in Services, but only if you stick to the goals of focusing on customer success and not your own, which brings us to the next point.

2.- Which metrics should be chosen?

The heartbeat of the business model is determined by the metrics chosen. The creation of a CX area must necessarily have measures and dynamics of their own, but that can also have an impact on the other areas, for example, Sales will experience enriched interactions with customers; Finance will have a close and anticipatory vision of the reason why a customer is likely, or not, to remain a customer; Services will be able to focus on the transactional aspects, but with a higher sense of customer sentiment.

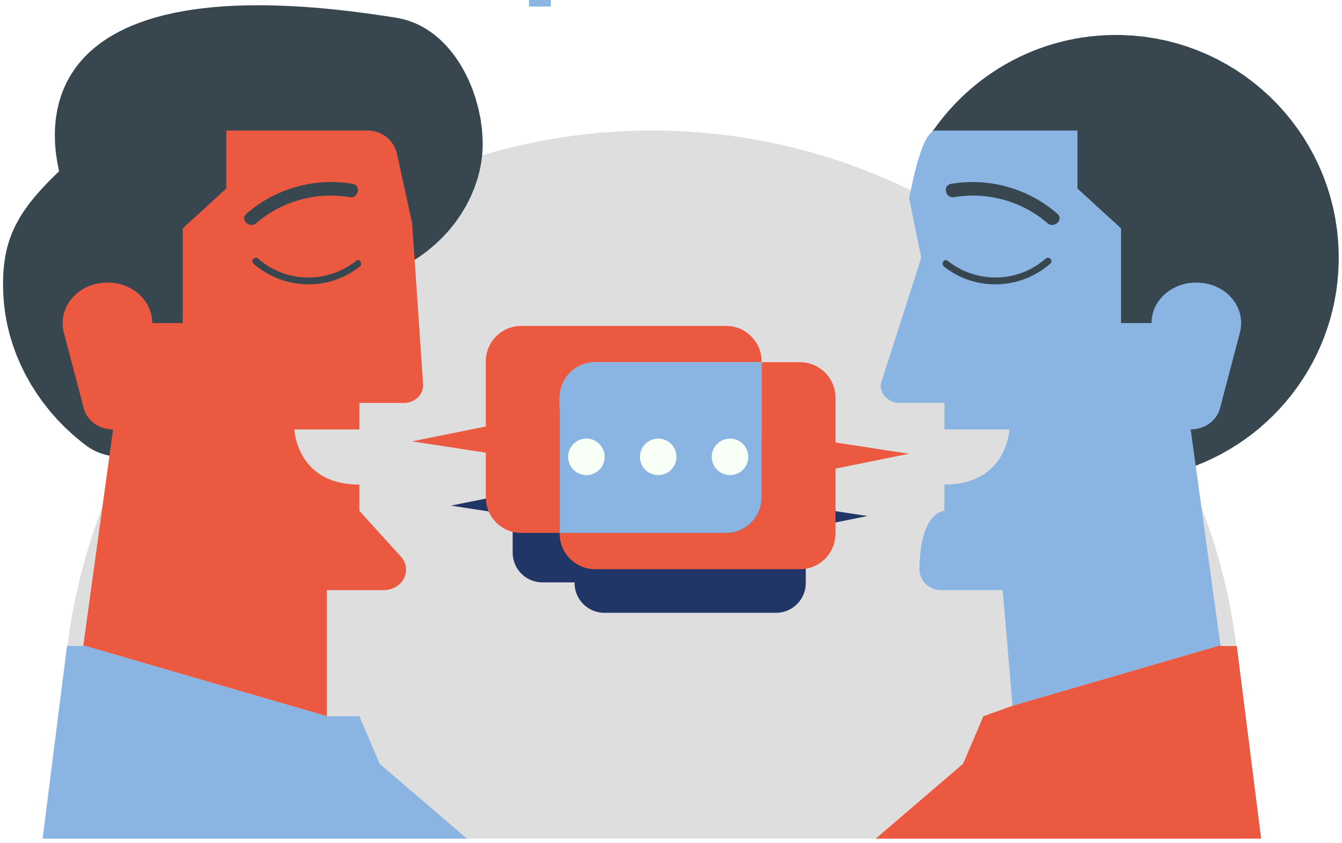
The fundamental metric of the CX area is the success of the users, as measured in their own metrics. No other metric is more important. Naturally, that creates an impact on the NPS (Net Promoter Score), the renewal rate, customer loyalty, among others, all of which are provider metrics.

Customer success must be the sole focus and raison d'etre. It has created new ways of working internally, it has affected compensation models, it has changed communication dynamics, and it has helped reassess the fundamental metrics of the organization.

The arrival of CX not only changes everything, but also affects traditional organizational dynamics as a whole.

Everything everywhere all at once. That's what it's all about.

Human Beings and their voice to enhance customer experience



Customer experience lies at the core of every organization. Today, companies don't just offer products or services; they provide added value—a complete experience. Every interaction with customers can either enhance or harm their perception of the brand. Placing the customer at the center of the strategy means addressing this transformation, which includes actions and emotions, exploring new edges, innovating, and evolving. It requires a keen observation of the various elements that impact, disrupt, and reinvent the way of doing business. One such element is empathetic communication, which takes shape, for example, through the voices of entrepreneurs and their collaborators.

"When we talk about the customer experience, what comes into play is the experiential, the approach, the trust…" says Nadia Simón, CX Regional Manager at OCP TECH. She adds that, currently, factors coexist that, until a few years ago, would not have been considered when setting up businesses.

How to convey the message correctly? What role does the voice play in this? These questions form the basis of a panel discussion led by Nadia Simón, featuring the valuable contributions of Customer Experience Consultant Pablo Marrone, and Vocal Coach Claudia Menkarsky.

Watch
the video here

The voice of the companies

Pablo Marrone believes that “today customers seek to feel that their needs are being heard and that they will be supported throughout the journey.” They agree that the way of doing business is changing. “Today, many companies offer similar products or services, and customers look for the distinctive elements. That’s more or less what happens when you go to a restaurant. Do we come back for the food? No, we return to where we had the best experience. And in this customer experience, the service provided by the waiter, the trust they inspire, their attitude, their way of communicating all play a role.”

For Claudia Menkarsky, “our voice identifies and defines us.” She believes that, to feel comfortable with our own voice, it is necessary to observe emotional management and to manage tones, pace, frequency, speed, and empathy. Only then is it possible to effectively communicate and make a significant difference.

The journey to manage our own voice and communication style properly begins when we become aware of our own breathing. “Our breathing flows in our voice and conveys our state of consciousness, our emotions, our energy. Through self-awareness, we transform ourselves to express what we want in the way we want.” Based on her expertise as a Vocal Coach, she highlights the opportunity to breathe deeply to reconnect: “Breathing regulates the nervous system, our heart rate, and makes us focus. By breathing deeply, we oxygenate ourselves; thus, we will always be able to find in that inspiration an internal connection that will help us regulate emotions and speak from the best of ourselves.”

She delves further: “All words are born from silence, so listening is the first instance from which we will be able to have that time of reflection and internalization to allow those appropriate words to emerge based on what we see and what we want to communicate and convey.” Every human being has their own way of speaking: “Each voice is unique and every time we speak, we convey our essence in a very particular and well-defined manner.” She states that finding one’s own voice is connected to the infinite essence of who we are, which is individual and also depends on energy and the encounter with the other.

Claudia Menkarsky adds: “Each voice has a light of its own, and what we give is unique—a glimpse into this personal multiverse that comes with a frequency, with an energy. It’s crucial for each person to find their own light, their own voice, their own consciousness to be able to communicate in the best way.”

Passion for work

Once we find our own defining voice, what is the secret to effective communication? “Being convinced of what we want to give, speaking passionately. Then, we will be able to communicate it effectively,” says Menkarsky. From Simón’s point of view, different elements come into play, such as interpersonal relationships, understanding the goal and mission, knowing where we are and where we are going: “In our case, the organizational structure is open and transparent. We promote kindness to address, for example, a colleague who cannot access a connection or who has a problem with a tool... it’s as simple as reaching out and offering help, and that is also a CX experience,” he adds.

For Pablo Marrone, customer satisfaction is the philosophy that envelops an organization:

"Some time ago, we used to talk about Total Quality, an all-encompassing concept. This is the same; it involves all areas." He adds: "Many times, when doing Customer Success consulting, the first thing you find is resistance to change. We must be willing to change. And also, be empathetic, have an understanding of the other person. Customer Success exists because there is another person on the other side of the counter in any given role. In our industry, we often tend to focus on technology and forget about that empathy, that need to communicate with the other."

Nadia Simón and Pablo Marrone agree that organizations currently recognize that the entire structure is focused on managing the best customer experience. Each employee, each area of the company is responsible for a part of that experience.

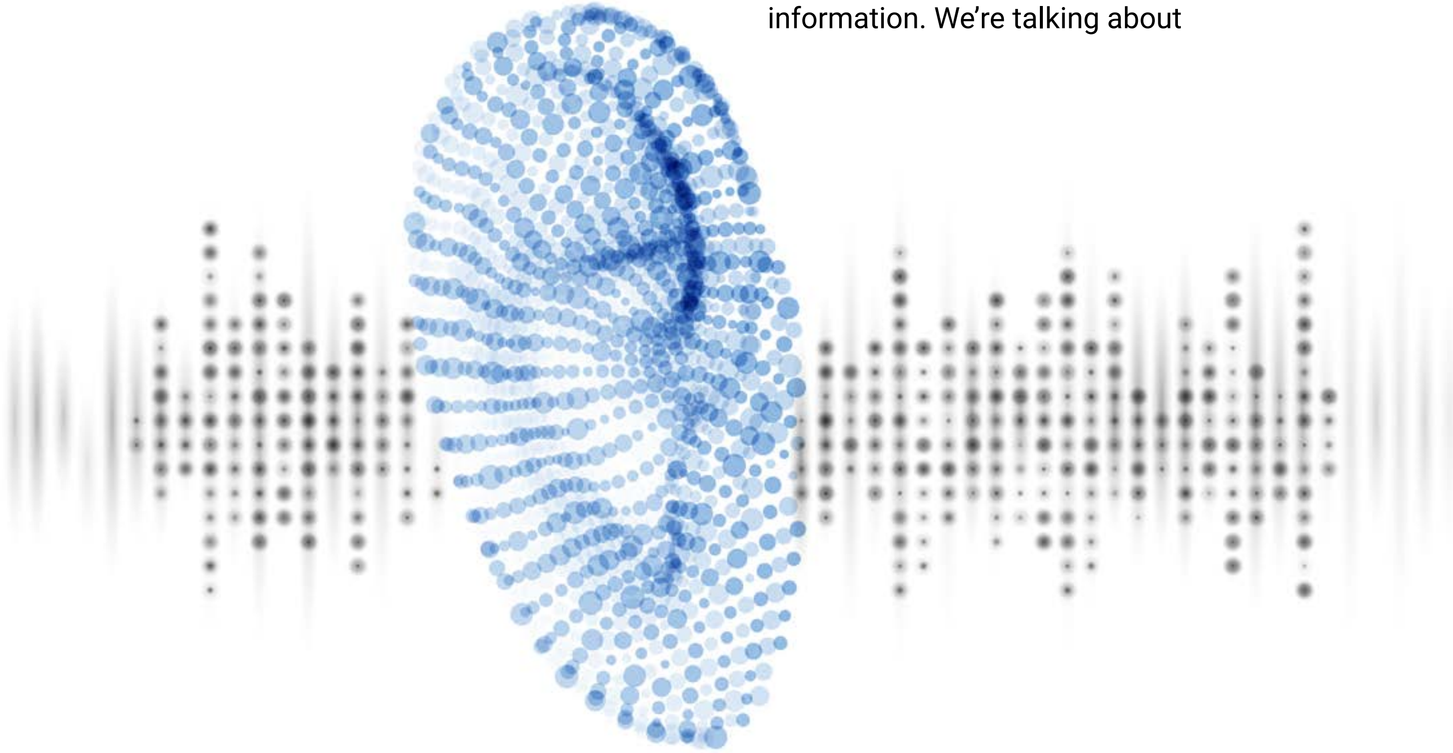
At OCP TECH, "the operation seemingly integrates with the customer's framework, and all areas feed each other. Our symbol is the infinity symbol, which is related to continuous monitoring. We have been promoting this culture for several years," says Nadia Simón. In the team, different profiles coexist, working as a whole: "It is our distinctive approach. When it comes to addressing the customer experience, we work a single team," she completes.

A trend or an evolving reality?

"From an organizational point of view, I think we are witnessing something that is far from being a trend. My opinion is that the Customer Success or the Customer Oriented Executive is going to be the leader to whom Sales, Product, Strategy, and Marketing will report," predicts Pablo Marrone.

Claudia Menkarsky adds that, amidst technology, humanization is imminent: "A renaissance of the human spirit is approaching, where technology will come to life not merely as a communication medium, but with the transcendence of conveying values and essential information for everyone. When it is at the service of human beings, it is wonderful because it reaches everywhere."

Nadia Simón emphasizes that once you've entered the Customer Experience world, it's impossible to approach customers in any other way. "I have been in the market for more than 20 years, and I believe that, these days, bonds can be formed in a different manner. It is possible to add value and change. Our work has a social impact. Every day we see kids from distant places gain access to communication... that connectivity turns on and we understand that we are changing someone's life, providing access to the basics of education and information. We're talking about



Nadia Simón
CX Regional Manager
at OCP TECH

Claudia Menkarsky
Vocal Coach

Pablo Marrone
Customer Experience Consultant

technology, but the impact from the social point of view makes a significant difference and motivates us to get up every day and say: 'Well, let's make things happen.' From my position and from the company's point of view, we truly make things happen, together with the team, which has a great commitment."

Therefore, the method consists of building the best possible connection with all the interested parties, investigating the best ways to convey and communicate, recognizing and managing one's own voice, taking breaks to reorganize, listen, understand, and then, establishing the best dialogue.

Bridging the gap

OCP TECH's challenge is to improve communication, integrate different profiles—both young and experienced,—and keep up with trends and demands: "We are aligned in this goal," says Nadia Simón, and focuses on the need to know how to listen to the different audiences, in addition to learning how to communicate,

Claudia Menkarsky adds: "What Nadia says is very interesting because, nowadays, there's a huge generational linguistic gap. It's not the same how we talk to a forty-year-old as how we talk to a twenty-five-year-old. Language plays a fundamental role; therefore, conveying a message clearly is key to achieve effective communication in any company."

Metaverse

META (beyond)
VERSE (universe)

The word metaverse is a portmanteau composed of the prefix meta, which comes from Greek and means "after" or "beyond", and verse which means "universe". It is a virtual and three-dimensional (3D) ecosystem in which users can interact with each other, work, play, study, conduct economic transactions, among many other possibilities. All of this occurs in a decentralized manner.

What makes metaverse possible?

Technologies such as blockchain, augmented reality, virtual reality, 3D, artificial intelligence, or the Internet of Things.

How can we participate?

Accessing this space is achieved through new interfaces such as smart glasses or haptic gloves, which allow us to fully use immersion capabilities in a sensitive manner. Additionally, blockchain and NFT (non-fungible token) technologies introduce units of value that can be exchanged through purchasing and selling.

The challenge

Going from “metaverses” —in plural— to “the metaverse” —in singular. Today, there is no single metaverse, since the different proposals are independent and disconnected from each other, behaving like isolated silos where the elements or experiences from one platform cannot yet be shared with others.

Key challenges to achieving this objective

- Achieving interoperability between different universes or platforms in order to be able to use avatars, currency, and experiences in different environments. In this sense, blockchain technology can contribute by proving the capability to own and transfer value without the need for third parties.

- Building highly secure spaces that protect personal data and transactions.

- Preserving the ethics of participants in the virtual space while developing experiences and activities with responsibility.

- Addressing legal matters that consider issues such as whether we will have the same rights and obligations as in the real world, or whether the same laws as in the physical world will apply.

- Recognizing the psychological challenge that this 3D environment poses for people who explore it..

- For brands, this could evolve into a new way of interacting with consumers through different immersive experiences, fostering the creation of a community with common values that encourages repeat interaction.

Web 1.0
hypertext - links.

Web 2.0
interaction - social networks.
Experiences in two dimensions.

Web 3.0
creation and exchange of digital assets
- NFTs - using blockchain technology.
Experiences in three dimensions.

Fun facts

- The word metaverse is 31 years old and was coined by Neal Stephenson in his 1992 science fiction novel Snow Crash, which envisions a virtual reality-based successor to the Internet.
- *The global metaverse market is predicted to attain $936.6 billion by 2030, at a Compound Annual Growth Rate (CAGR) of 41.6%, according to Grand View Research, Inc.*
- One of the first legal encounters with this new universe took place in New York, when the Court ruled in favor of the company MetaBirkin, which had alleged trademark infringement. In the case, the company claimed that virtual bags of the “Birkin” model were being sold in NFT format.

5 movies to understand the metaverse

Free Guy (2021) - USA
Director: Shawn Levy

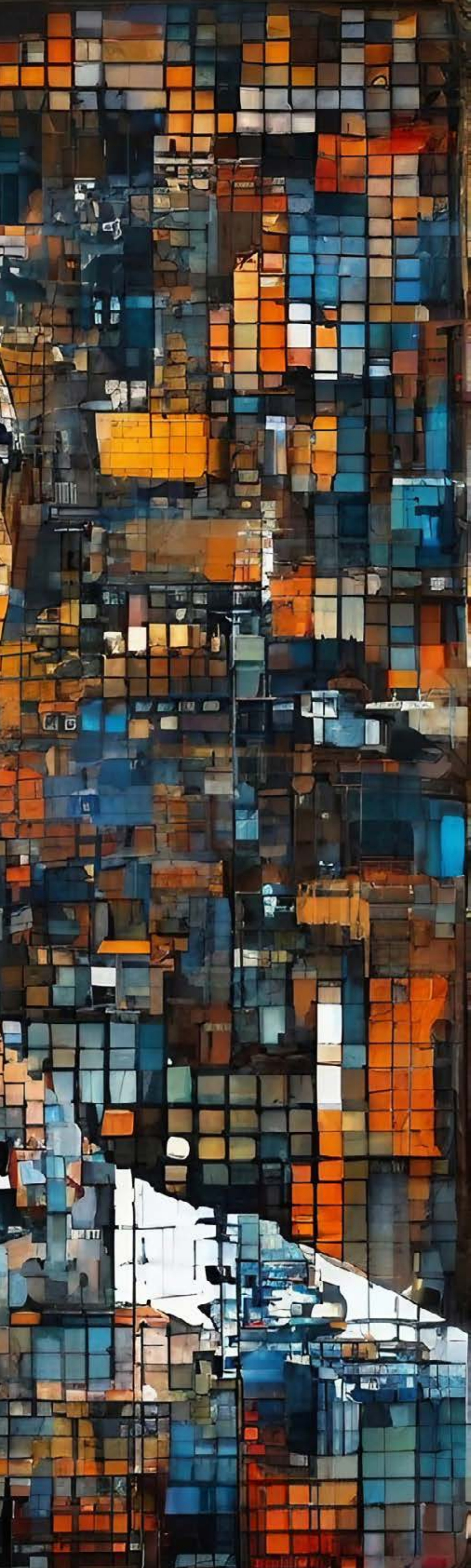
Ready Player One (2018) - USA
Director: Steven Spielberg

Total Recall (1990) - USA
Director: Paul Verhoeven

Snow Crash (2014) - USA
Director: Joe Cornish

eXistenZ (1999) - Canada
Director: David Cronenberg

The possibility of maintaining a consistent identity across various parallel universes will not be merely an aesthetic preference. Interoperability is desirable in several ways, for example, to enable the use elements acquired in different areas, to verify our identity and behavior, and to preserve our history, just as it occurs in the physical world.



Art by IA

Generative artificial intelligence is making significant strides. With responsible use and adaptation to the relevant context, it can help or complement our knowledge.

We asked Clipdrop by Stability AI, to create a digital piece for us that illustrates the man immersed in his future thoughts, yet established, anchored, connected to his city.

This is the result. What do you think?

Interview with

Leonardo Scatturice
Founder and CEO, OCP TECH

by **Flor Palazzolo**

Flor: Leonardo, thank you for taking the time to participate in this first edition of our annual publication. In a sense, we are celebrating, aren't we? *Laughs*.
To begin this interview, I would like you to share a little about yourself. What can Leonardo tell us about Leonardo?

Leonardo Scatturice at OCP TECH headquarters, Miami, FL.

Leonardo: What a start, Flor! It's true, we are celebrating. This annual publication is a perfect kick-off to connect and discover the essence of OCP TECH. Approaching your question, I think it is certainly complex to talk about myself. Years ago, I might have responded with qualifiers and big words, but now, with some experience, I would say that the answer lies in looking back at my actions. Something that has characterized me over the years is the constant need to open new paths and strengthen my vision of the future. In short, I believe that every human being seeks to empower themselves and feel part of something greater, and thus, in some way, impact reality and leave their mark. I have always believed in the ability of technology to transform lives and improve companies... somehow, the existence of OCP TECH and its constant expansion is an indicator that speaks about me more than anything else. Having founded this company speaks of a Leonardo who seeks to encourage a team to make a difference, and that is something I truly identify with. I would say that teamwork was one of the key factors in both my personal and professional development.

Flor: Regarding the last point you've mentioned, you are certainly widely recognized as a visionary leader, but we both know that this responsibility comes with challenges. Do you have any counterbalance in your role as a leader? What is it?

Leonardo: Sure, Flor. Being a visionary leader is exciting, but it is also challenging. I believe a significant counterbalance is maintaining the right balance between innovation and stability. We are always looking for new ways to grow because that represents the very essence of the company, but we must also ensure that our foundation is solid and that our teams are aligned with our vision.

"We are catalysts of change and believe in making a positive difference in people's lives".

Flor: Now that you've mentioned it… your vision for OCP TECH was expansive; the company has developed a strong presence in several Latin American countries. What is the main challenge posed by this expansion?

Leonardo: The expansion into Latin America has been an exciting milestone for OCP TECH. The main challenge lies in understanding and adapting to the different cultures and markets in the region. Each country has its own needs and challenges, and we must be flexible and agile to provide solutions that adjust to every scenario. It has been an arduous journey, where many people have worked very hard and there is still more to be done... I think we are on the right track, at the close of this edition we already have a presence in 15 countries. However, our company's vision doesn't stop there, so we will advance on the expansive path.

Flor: Absolutely. Now, allow me to delve into areas that some might call metaphysical... tell me a little about the soul of OCP TECH. How would you describe the essence of the company?

Leonardo: The soul of OCP TECH is impact engineering, through constant innovation and knowledge. We are a passionate team focused on finding advanced technological solutions for our customer. Our essence lies in creativity, collaboration, and commitment to excellence. We are catalysts of change and believe in making a positive difference in people's lives.

Flor: That sounds truly inspiring. Now thinking in more tangible terms, what is the body of OCP TECH like?

Leonardo: Certainly, the body of OCP TECH consists of our employees, customers, and partners. We are a global, diverse, and highly skilled team working together to provide comprehensive solutions. Our customers and partners form the foundation of our growth and

***Andrés Quinn**, COO, OCP TECH, and*
***Leonardo Scatturice**, CEO, in constant dialogue about how to bring innovation closer to their customers.*

success. They are a fundamental part of our body, and we are always looking for ways to strengthen these relationships in the long term.

Flor: At OCP TECH, one of our core values is to be a customer-centric organization. What does this concept mean to you?

Leonardo: Being a customer-centric organization is essential for us. It means that we are focused on our customers at every step. We carefully listen to their needs, desires, and challenges, and create solutions that benefit them. Our approach is to build long-term relationships, provide exceptional service, and exceed their expectations. In today's highly competitive market, the best strategy is to return to the customer's needs, to their reality. Ultimately, the greatest added value that our service can provide is the understanding that it is designed based directly on their real needs. We focus on their business requirements, proactively propose technological solutions, and through a mature CX practice, we guide them through the entire cycle of efficient use of technology.

Flor: To sum it up, going back to the start where you told us about your plan to build for the future, where is the entrepreneurial Leonardo looking these days?

Leonardo: The entrepreneurial Leonardo continues to look towards the future with great enthusiasm and determination. Our focus is on continuous expansion, constant innovation, and taking OCP TECH to new horizons. In today's world, these new horizons must find us more connected than ever, developing markets where the customer takes steps forward with us, standing firm. It is our responsibility to be the guide to this new space, seeking feedback on new experiences, ideas, and technologies. To be honest, Flor, I am excited about what the future holds for us, and I trust that together we will be able to continue generating the significant impact that the technology universe needs.

OCP TECH

global IT

Fraud and Cybersecurity

There are scenarios where the interests of areas such as Cybersecurity and Fraud Prevention diverge due to their specific needs and the pursuit of quick resolutions, which may not necessarily be the most suitable for the protection of personal or sensitive data. Is it possible to strike a balance between the requirements and needs of Fraud Prevention and those of Cybersecurity? Fabio Sánchez, Director of Cybersecurity Practices at OCP TECH, and Eric Balderrama, Lawyer and Co-Founder of Trully, approach the issue from different angles, including that of the issuer of the payment method, the seller/store, and the end user. They also present some ideas to streamline processes in these areas. Here are some excerpts from the conversation.

Context

Our current environment is moving towards digitalization, eliminating the need for physical presence in transactions. This shift requires fraud prevention teams to verify user identity through alternative methods rather than the traditional one, where users physically appeared to open an account or conduct a transaction. Many organizations have adopted biometric authentication for account openings and MFA (Multi-Factor Authentication) for transactions, such as a mobile token or an SMS with an OTP (One-Time Password) code. However, there are scenarios where criminals manage to evade or

Watch the video here

manipulate these digital processes by conducting fraudulent activities such as identity theft, account theft, or abuse of business logic, among others.

Fabio Sánchez emphasizes: “In Cybersecurity, the priority is to safeguard the confidentiality, integrity, and availability of the information being processed. A common advice for end users is to avoid sharing personal information such as names, credit card details, and addresses to minimize the risk of it being used in fraud. However, this significantly hinders usability, practicality, and simplicity in operations. Striking the right balance between security and usability is a major challenge: when to share and when not to share such information, and what to disclose.”

“I believe the issue extends to a higher level, a step beyond. Generally speaking, the vast majority of cybersecurity and fraud teams do not align; they do not communicate. Even though they belong to the same company, they often operate in silos: Cybersecurity focuses on meeting regulatory compliance associated with the area, while Fraud Prevention aims to strike a balance between preventing fraud and preventing sales. Why? Because instead of making the purchase or transaction process frictionless for the individual, additional barriers or controls are introduced for protection, often hindering the sale. The current environment reflects a lack of communication and the absence of defined standards and guidelines between both areas,” responds *Eric Balderrama*.

“In a context where everything tends to be authenticated remotely, it becomes more complex for the fraud prevention team to identify who is who. How do we verify that Fabio is indeed Fabio? Commonly used methods include identification and a selfie. Even though some systems, known as KYC (Know Your Customer), operate during the origination process, they are not enough. While there may be regulatory compliance in place, it doesn’t necessarily provide an effective barrier against fraud. Later, when customers initiate transactions, how do we confirm that Fabio is truly Fabio? There are different methodologies, such as behavioral analysis. For instance, if Fabio usually makes purchases on four or five e-commerce platforms and suddenly there is a transaction elsewhere with a very high cost, it is prudent to request a second authentication factor. This does not necessarily involve sending a photo of the card and of oneself. This is where the fraud prevention process comes into conflict with cybersecurity for information protection, and where the lack of communication between Cybersecurity, Fraud Prevention, and even AML or Compliance becomes evident,” explains *Eric Balderrama*.

“The objectives of both areas are different. From a business perspective, one aims to prevent fraud or identity theft without impacting sales. “Cybersecurity is responsible for protecting information through the implementation of controls and security layers, which may potentially make origination and transaction processes increasingly difficult,” says *Fabio Sánchez*.

“It is also crucial to understand the practices that are already implemented and widely adopted.

Most personal data protection laws in countries are based on ECLAC (Economic Commission for Latin America and the Caribbean), which established a model law for personal data. This does not mean that a company is legally restricted from requesting a photo of your card or your ID; they can do so. However, ideally, they should have a publicly accessible privacy notice where they outline the types of sensitive data they will request, the treatment they will apply to that data, and the duration for which that information will be stored. For instance, some digital ticket-selling platforms lack these processes and prompt users to “send a photo of your ID and credit card for validation.” This can be reported. In each country, there are different channels for reporting: in Argentina, there is Consumo Protegido (Prior Conciliation Service on Consumption Relations); and in Mexico, there is PROFECO (Federal Consumer Protection Agency). Users should exercise their rights to compel these companies to comply with regulations. On the other hand, understanding the perspective of fraud teams offers an explanation for their actions: it’s a practice that has already been implemented. Let’s briefly imagine being part of a fraud prevention team. How do we validate that a person is truly the one initiating a transaction? How do we do it easily, quickly, and simply? And then, we should also ask: Is this the most effective method? Are there alternative, more accurate approaches?" - *Eric Balderrama*.

Responsibilities

Issuer of the payment method

Stay current with technology to implement solutions that streamline tasks for both sellers/ stores and end users.

Seller/Store

Implement two-factor authentication technology.
Promote personal data protection policies.
Keep internal systems up to date.

Align the Cybersecurity and Fraud Prevention areas, promoting their communication and balancing their objectives.

User

Protect personal information and exercise caution when sharing it.

"By implementing alternative methods of customer verification and identification, companies can avoid requesting users to provide more information than needed. This also eliminates the need to store personal information and concerns about how to protect it. By applying alternative methods to verify authenticity, I believe we make life easier for users and make their shopping experience more pleasant," explains. *Fabio Sánchez*.

"At the company level, it is also important to implement a robust data governance system. As Fabio mentioned, there is often user information scattered across multiple locations, such as databases, shared directories, or a collaborator's computer. When users exercise their rights, for example through ARCO (Access, Rectification, Cancellation, and Opposition) Rights, the company will delete only the data registered in the database, but it will remain accessible in other locations. This poses a challenge to the protection of the owner's personal data," adds *Eric Balderrama*.

Possible Technological Solutions

OTP (One-Time Password), such as 3DS (Secure): Depending on the transaction amount, a token is sent to the buyer's mobile phone, then they enter the OTP into the transactional flow, and that's it!

Dynamic CVV: Dynamic CVV: In digital card scenarios, the three validation digits of the VISA or Mastercard credit card, or four digits in the case of AMEX, change at defined intervals. This causes the CVV to function as an OTP.

Chip + PIN: For in-person channels with a physical card. The PIN acts as a second authentication factor, since something I have (the card) aligns with something I know (PIN).

Validation using a small transaction amount: Only the user has access to their account to identify the exact amount of the transaction. "I have implemented it, and the cost is very low. It serves as an excellent alternative. A positive outcome from this conversation could be to raise awareness about this solution. Instead of requesting the user's ID and credit card, a nominal charge of a few cents is applied to the user's credit card. The user then confirms the exact amount of the charge, and upon verification, the transaction is validated," suggests *Eric Balderrama*.

Recommendations

Companies

Implement comprehensive security measures at the fraud prevention level. While maintaining KYC (Know Your Customer), strengthen the origination process with alternative data and, if possible, leverage collective fraud prevention networks. Reinforce the user's transactional process with OTPs and tokens, among others, to authenticate and validate operations.

Understand how buyers behave. If they always use certain credit cards and there is a sudden change in payment methods, validate the transaction to ensure its legitimacy.

Align communication between Cybersecurity and Fraud Prevention areas to implement controls that streamline user experience while safeguarding information.

- Introduce alternative methods that eliminate the need for requesting personal information, supported by available technologies that simplify the process.

Users

- Assume responsibility for protecting personal data.

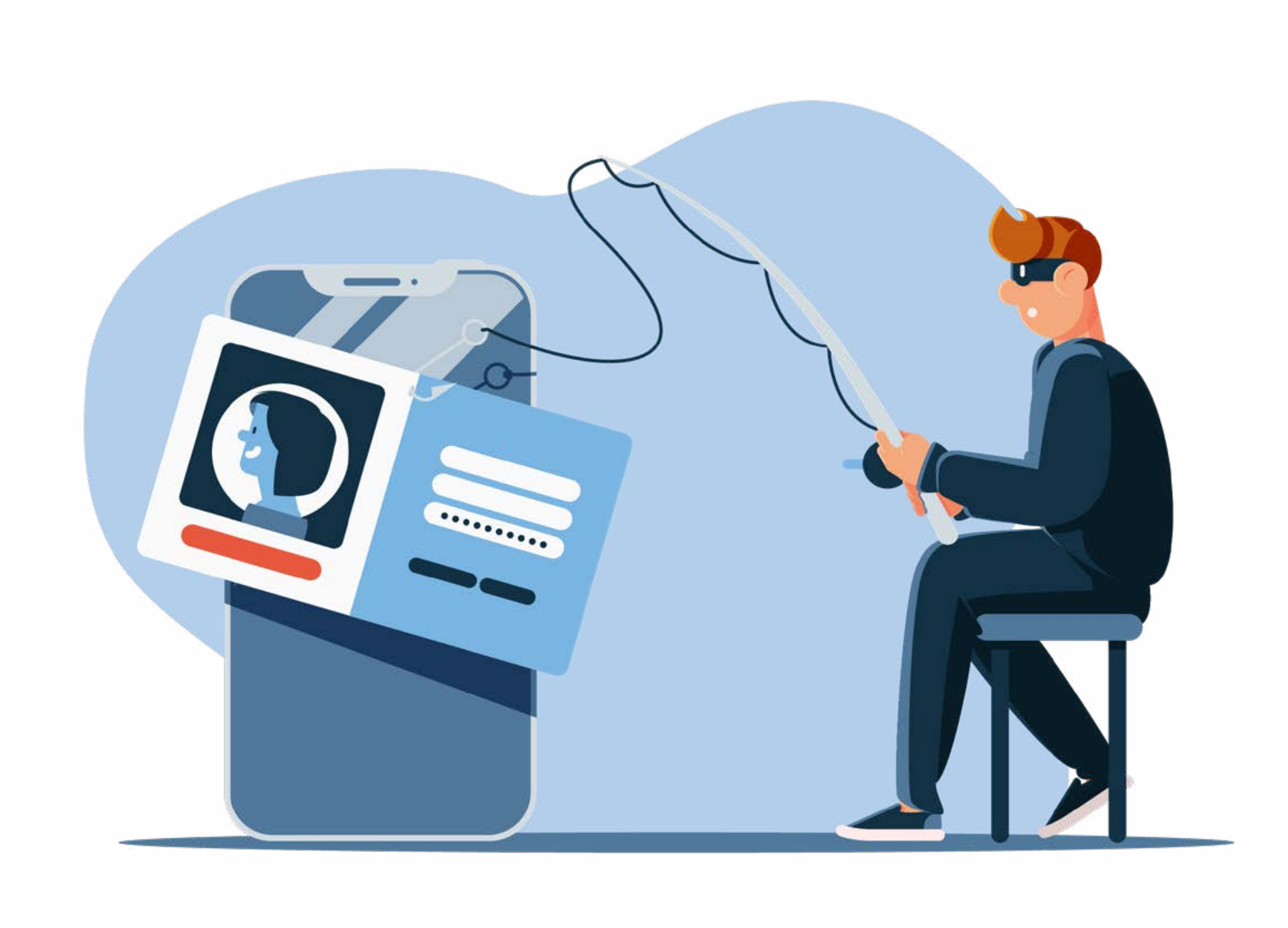
- Dedicate time to regularly review account statements for various cards.

- Familiarize with privacy notices, and terms and conditions of platforms, or use a GPT service for summaries: understand what data we disclose, its intended use, and the policy and retention period. Also, explore available options for data elimination.

- Enhance security by implementing second authentication factors.

- Exercise control over access and verify it regularly.

- Exercise caution with the information we disclose and avoid normalizing the process of sharing sensitive data.



What we talk about when we talk about Personal Data

There are regional regulations in several countries. In LATAM, there is also the Model Law on the Protection of Personal Data established by the Economic Commission for Latin America and the Caribbean (ECLAC), which serves as a guide and reference for the countries in the region in the development of their national data protection laws. Although the Model Law is not inherently binding, it has been used as a basis for creating and revising data protection legislation in several Latin American countries.

In each country, the definition of “personal data” may vary; however, in general, they include:

Identification data: First name, last name, identification number (such as ID card or passport number), date of birth, gender, nationality, among others.

Contact information: Home address, telephone number, email address, or other personal contact details.

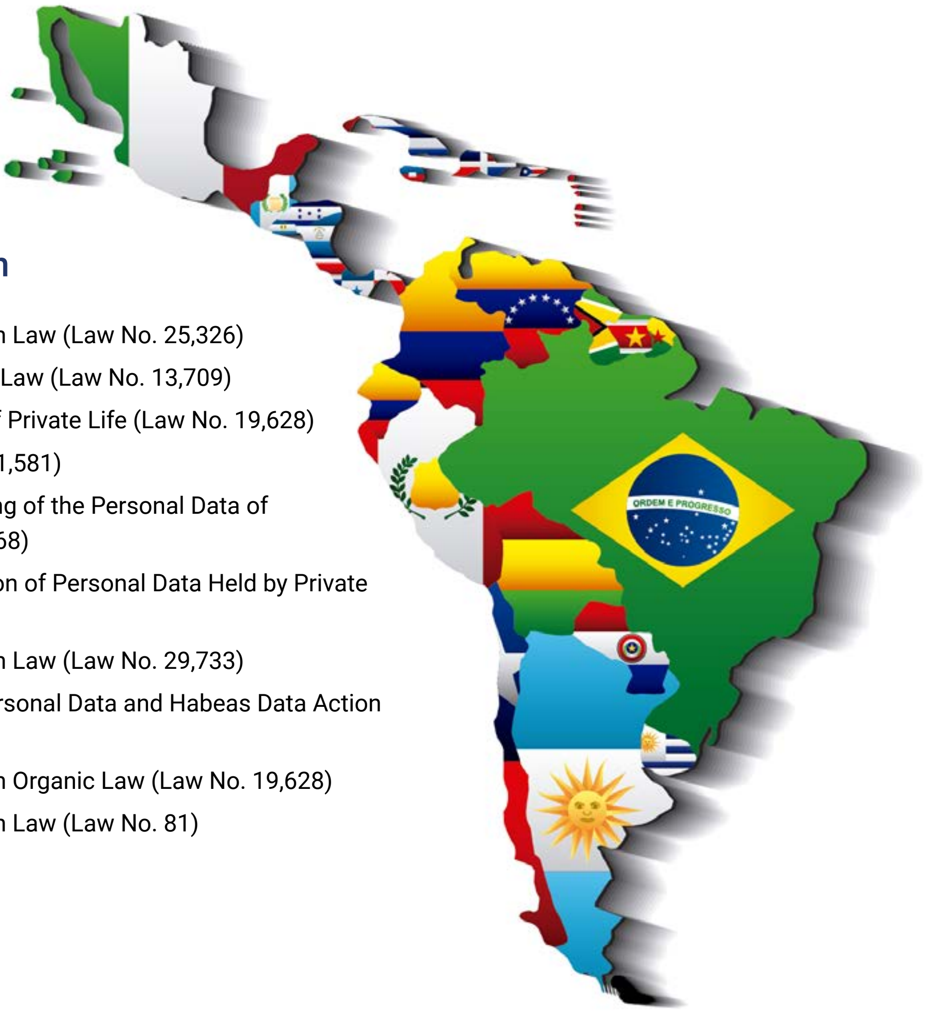
Sensitive data: Information relating to an individual’s health, racial or ethnic origin, religious or philosophical beliefs, trade union membership, sexual orientation, criminal records, among others.

Financial data: Bank account number, credit or debit card numbers, history of financial transactions, income, debts, among others.

In order to operate efficiently within various organizations, the teams in the Legal, Cybersecurity, and Fraud Prevention areas have the responsibility of internalizing and reviewing the legislation applicable in each country. This includes understanding how it addresses aspects related to personal data, such as informed consent, legitimate purpose, data quality, information security, as well as the responsibilities of those involved during data processing, storage, transmission, and destruction.

Legislation in Latin American Countries

Country	Law or regulation
Argentina	Personal Data Protection Law (Law No. 25,326)
Brazil	General Data Protection Law (Law No. 13,709)
Chile	Law on the Protection of Private Life (Law No. 19,628)
Colombia	Statutory Law (Law No. 1,581)
Costa Rica	Protection in the Handling of the Personal Data of Individuals (Law No. 8,968)
Mexico	Federal Law on Protection of Personal Data Held by Private Parties
Peru	Personal Data Protection Law (Law No. 29,733)
Uruguay	Law on Protection of Personal Data and Habeas Data Action (Law No. 18,331)
Ecuador	Personal Data Protection Organic Law (Law No. 19,628)
Panama	Personal Data Protection Law (Law No. 81)



```
<stdint.h>
int argc, char **argv) {
nt64_t src = argc;
nt64_t dst;
_asm__ volatile(
        "lzcnt %1, %0\n"
        :"=r"(dst)
        :"r"(src)
        :"cc"

return (int)dst;

    #define ASM_VMX_VMREAD_RDX_RAX    ".byte 0x0f, 0x78, 0xd0"
    static __always_inline unsigned long vmcs_readl(unsigned long field)
    {
        unsigned long value;
        asm volatile (__ex_clear(ASM_VMX_VMREAD_RDX_RAX, "%0")
                      : "=a"(value) : "d"(field) : "cc");
        return value;
```

Geopolitics and Cybersecurity

In the digital era, threats to the security of countries find a new battleground: the cyberspace. Simultaneously, another dimension is added to political strategy. How are the leading countries moving forward?

The threat of attacks on countries continues to fuel a race against time among the world's major powers to develop the most sophisticated weapons. However, in the 21st century, one of the scenarios par excellence is cyberspace, and the aim is to develop an arsenal of cyber defenses. Today, information reigns supreme, and protecting it is essential. Therefore, the geopolitical dimension is a strategic chapter in cybersecurity.

Major powers allocate significant resources to ensure national security and safeguard their information systems, striving to stay one step ahead of threats, which evolve at the pace of constant digital transformation processes.

ublic abstract class AbstractA implements
protected abstract void doStuff(X x);
protected abstract void doMoreStuff(
public void execute() {
X x = getX();
doStuff(x);
Y y = getY();
doMoreStuff(x, y);
}
// getX(), getY()

Global Vulnerability

Viruses and malware, phishing, denial-of-service attacks, password attacks, and ransomware are some of the most common threats used by malicious individuals, corporate spies, or criminal organizations. According to data from Cybersecurity Ventures, a reliable source on the global cyber economy, it is estimated that by 2026, the global cost of cybercrime will amount to $20 trillion (USD).

In January 2023, the World Economic Forum (WEF) published its "Global Cybersecurity Outlook 2023", in collaboration with Accenture. The report, based on a survey of 117 global leaders from 32 countries and 22 industries, reveals that 91% of respondents believe a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years. Additionally, 43% stated that a cyberattack is expected to occur.

With global vulnerability just a click away, the industry faces significant challenges to build a safer environment for individuals, companies, organizations, and governments. The global mix, marked by cyberattacks that know no borders, requires an additional element: international cooperation.

Many countries are rising to the occasion by implementing programs to minimize risks and enacting laws to enhance cybersecurity safeguards.

Below are some examples.

Singapore, the United States, and Spain

In the latest edition of the Global Cybersecurity Index, published by the International Telecommunications Union (ITU), a specialized agency of the United Nations (UN), it is reported which countries have the best cybersecurity worldwide.

The efforts of Singapore stand out, as the country has implemented strong policies, regulations, and training programs to protect its critical infrastructure and promote cybersecurity awareness.

The United States has taken measures to protect its infrastructure, strengthen data security, and promote cybersecurity education. The Cybersecurity Information Sharing Act (CISA) allows the exchange of Internet traffic information between the Federal Government and technology companies. Local regulations in some states penalize companies for cybersecurity failures. Companies proactively invest in cybersecurity to avoid reputational and financial loss.

The top 3 also includes Spain, which has a national strategy and a series of initiatives to protect its critical infrastructure and promote public-private cooperation and training. The country has robust regulations regarding data protection.

United Kingdom, Estonia, China

The United Kingdom has numerous laws regarding cyber aspects. Notable among them are the Data Protection Act and the Privacy and Electronic Communications Regulations for telecommunications service providers. Significant penalties are imposed on negligent companies. The government addresses this risk through a National Cyber Security Center (NCSC), responsible for protecting critical services, managing major incidents, and enhancing security through technology and guidance.

Estonia approaches cybersecurity as part of comprehensive security plan within the context of the North Atlantic Treaty Organization (NATO) and national security. The country has implemented a digital identification and identity system for each citizen that enables access to online public services. Moreover, it seeks to apply international law to conflicts.

The People's Republic of China has implemented a cybersecurity project based on increased state intervention. Their estimates reflect the idea of a common destination cyberspace community, whose core is based on respecting the cyber sovereignty of each nation and the need to establish guidelines for cyberspace through extensive intergovernmental cooperation.

Development and Investment

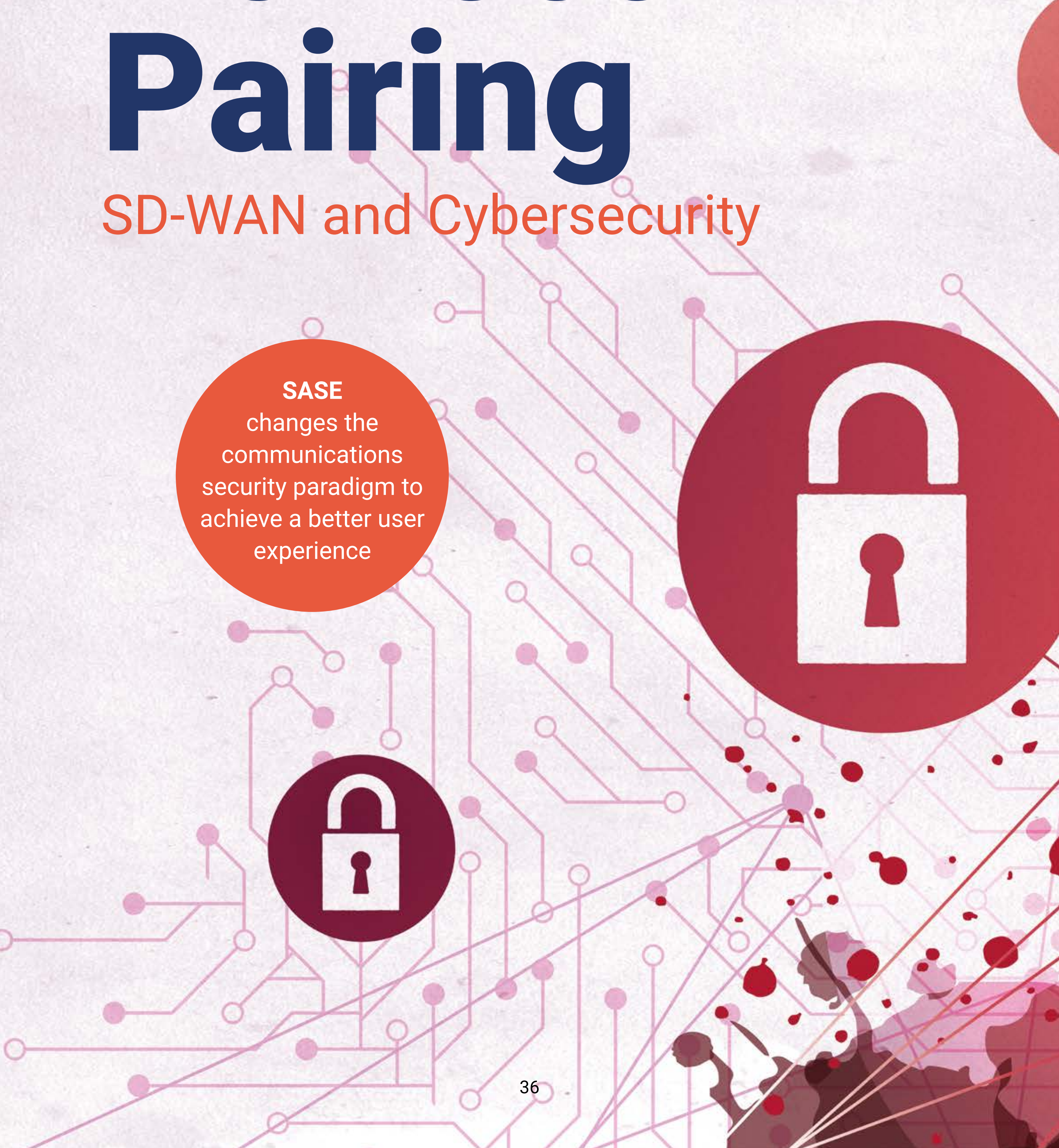
Denmark, Finland, the Republic of Korea, New Zealand, Iceland, Sweden, Australia, Estonia, the Netherlands, and the United States led the top 10 e-government in 2022, according to data from the UN Global Innovation Index. Furthermore, the European Union enacted the Cybersecurity Act in June 2019, which strengthens cybersecurity measures for digital products, services, and processes across the EU.

What do all countries updating in this area have in common? Digital Maturity. They show a commitment to digital innovation; they foster accessibility and inclusion, citizen participation, and service delivery, such as digital identification or online tax services; they promote cybersecurity, data privacy, and relevant legislation; they encourage international cooperation and exchange; and last, but not least, they invest in cybersecurity to support the development and innovation of companies and societies.

Countries in general, including those in Latin America, are gradually adapting laws and regulations related to cybersecurity to align with the fast-paced digital world. However, there is still much to be done.

Perfect Pairing

SD-WAN and Cybersecurity



SASE changes the communications security paradigm to achieve a better user experience

The right wine can turn an exquisite meal into an unforgettable experience. That is what culinary pairing is all about, a practice that is currently booming and aims to create new sensations, both in tasting the food and the accompanying beverage. And while finding the perfect match is not easy, experts can recommend combinations that work wonders for the most discerning palates.

In the realm of technology, traditional security systems are no longer sufficient in today's era of digitalization, remote work, and multi-device connections. As users connect from various locations and access sensitive data in the cloud, the need to enhance application performance and bolster network security becomes evident. With digital transformation, security shifts to the cloud. Thus, the demand for converged services arises, with the goal of simplifying complexity, enhancing speed and agility, enabling multi-cloud networks, and protecting the new architecture.

So, another example of a successful "pairing" is created: Secure Access Service Edge (SASE), a network architecture that intelligently directs traffic to the cloud and performs advanced security inspection through the combination of SD-WAN (Software Defined Wide Area Network) with cloud-native zero-trust security features. In this way, S-WAN and Cybersecurity affirm their commitment by providing a direct and secure access journey which connects users, systems, connection points, remote networks, and applications.

It focuses on optimizing connectivity, protecting data, and streamlining operations by offering comprehensive security for both companies and users; therefore, protection is ensured regardless of work location.

SASE Experience

To embrace the SASE proposal, it is essential to establish a strategy to identify the applications that can migrate to the cloud, secure the data, transform the infrastructure, and train the team to act accordingly.

With its technological architecture, companies can enable more secure mobile and remote access; reduce costs and complexity; limit access based on user identity, device, and application, as well as increase the effectiveness of security personnel and network through centralized management, among other functions.

According to experts, the goal can be summarized in the concept of the “3 Cs”:

- **Connectivity:** ensuring that any user, device, or application can connect automatically, simply, and securely.
- **Control:** implementing the “zero trust” concept to allow access to those devices that adhere to the established parameters.
- **Convergence:** facilitating the coexistence between agile and secure connectivity.

Remote work and digital transformation have changed the security perimeters offered by closed office environments, leading to evolving cybersecurity needs. It is in this context that SASE emerges.

The Cybersecurity Cold War

In this article, the author talks about the complex web of cyber attacks and how to protect yourself from threats in real time.

by **Fabio Sánchez**
Director of Cybersecurity Practices, OCP TECH

Advances in cybersecurity are happening faster than in other information technology (IT) industries or sectors, driven mainly by a hidden war economy similar to that of the Cold War of the 1990s. This Cold War in cybersecurity, which has been going on for some years now, is not fought between countries, but is waged by well-organized groups of cyber terrorists who have diverse objectives and push technology companies and service providers to delve deeper into cyber defense, innovate, and develop services and solutions focused on identifying and protecting against a number of increasingly sophisticated threats. At the same time, the use of cloud services is growing, as well as the volume of data generated daily and the access from highly interconnected laptops and mobile and smart devices.

It is no coincidence, then, that in terms of cybersecurity all analogies and metaphors point to war scenarios, which place us in a purely defensive stance against invisible attackers in a digital terrain that has expanded at a dizzying pace. Faced with this reality, it becomes more difficult to defend the borders and place controls on Internet ingress and egress, and for many organizations, it has become uncharted territory, even within their own spheres. Many of the actions and solutions in the market are aimed at helping organizations gain visibility and understanding of what is happening in this environment of digital mountains and valleys, very similar to that of the revolution we faced at the beginning of World War II, when the introduction of radar system proved to be a real game-changer. The radar system provided the military with an unprecedented ability to detect and track enemy objects at much greater distances than ever before. Similarly, cybersecurity solutions focused on providing visibility and observability have offered a new perspective of the scenario and surface of action, changed the rules of the game in the digital war, and provided the ability to recognize attacks in real time.

The truth that is stranger than fiction

However, the scenario would not remain unchanged for long, since the very speed and diversification of the attacks required greater ingenuity and agility to respond, and artificial intelligence would have much to contribute. Since its beginnings in the 1950s and throughout its evolution at the beginning of the 21st century, artificial intelligence has offered mathematical prediction models that provided information for threat detection and analysis. Nevertheless, these capabilities were limited to First World governments with very high computing capabilities. It was not until a decade later when new reinforcement learning methods

and convolutional neural networks, together with affordable computing capabilities, paved the way for the new revolution we are currently experiencing. Today, it is common to find solutions in the market that claim to have used artificial intelligence in favor of cyber defense. There are many methods and various areas of application, ranging from behavioral analysis—based on predictive mathematical models with unsupervised machine learning for the detection of anomalies and micro-anomalies caused by stealthy attackers and stealthy malware, which can infect computers and servers, thus slowly exfiltrating information for months without being detected—to autonomous response to port blocking and packet filtering that responds within milliseconds to the onset of an attack, before it can penetrate or inflict damage on a corporation's internal network.

The new war is undoubtedly being fought between machines. Human beings are no more than mere spectators in the daily conflict, far from the armed robots crushing skulls that science fiction predicted in books and movies a few years ago. This war is being fought before our eyes and we are not seeing it. It is happening at an imperceptible speed.

A new era has arrived with the democratization of artificial intelligence: today, anyone has the access to this technology in their fingertips, enabling them to generate codes and create fake internet pages, new viruses, and malware. The proliferation of new methods and attacks will be exponential in the coming years, targeting both ordinary users and small organizations—which had previously gone unnoticed or unappealing to cyber attackers—as well as much more aggressive attacks on large organizations.

The way we help both small and large companies face this challenge and confront this war will determine their future and survival. In the years to come, neither economic nor health crises will determine the end of a company. The crisis of the invisible cyber war being fought will determine who survives and how long, and survival will depend on how well-prepared they are to respond and recover quickly.

Tactics and strategy

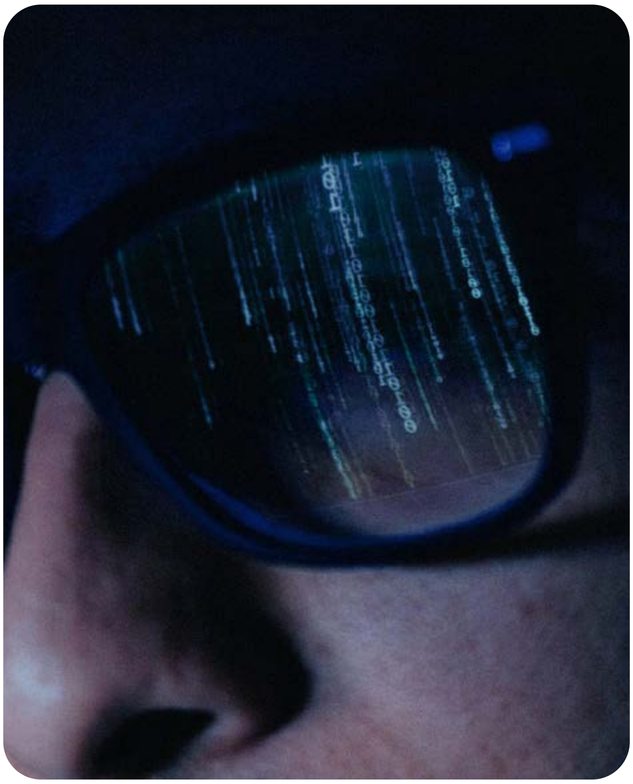
How to prepare and how to assess the status and maturity is one of the challenges that we are facing today at OCP TECH in our effort to help companies determine their weaknesses while giving advice on architectures based on the size and raison d'être of the organization, both in hybrid and full cloud environments. In the first stage, we focus on dimensions that are obvious and, at the same time, overlooked, such as identifying, protecting, detecting, responding, and recovering.

Identification involves implementing a process and platform for the recognition of information assets, software, and hardware that must be protected. They must be categorized according to the importance, criticality, and confidentiality of the information they handle. By achieving this visibility and management, organizations will be able to move forward and allocate resources to detection and protection. Otherwise, they will be blind to the risk, and recovering from a cyber attack will be very challenging.

The detection stage involves the use of segmented detection platforms to discover loss or movement of information within the internal network and public clouds. Its purpose is to find movements and abnormal user behavior that could compromise credentials and access, thus allowing cyber attackers to permeate the organization seeking a pathway towards critical services.

The protection of individuals can be achieved through awareness campaigns and training in cybersecurity, as well as with tools to safeguard their access through identity governance focused on individuals and their role in the organization. This also involves an appropriate management of highly privileged accounts and access to critical platforms of the organization, as well as the management and governance of information and data, both in personal user devices and cloud-based database servers in either data centers or third-party repositories, and the transfer of that information to and from cloud environments, internal networks, and the Internet.

By measuring capabilities and working towards growing in each of these areas, it will be easier to prevent unauthorized access to individuals, data, software, and hardware, regardless of the size of the organization, and, therefore, we will be closer to winning this cyber war of the new century, battle by battle.



A day in the life of ...

Illustration by
Santiago Guerrero

… Andrés Quinn

COO, OCP TECH

Who can resist the fantasy of living someone else's life for one day? In our conversation with this renowned leader of OCP TECH, we delve into the world of a Chief Operating Officer. We invite you to discover his vision, experience, and approach to managing a role that requires a balance between expansive thinking and strategic action.

What does an early morning alarm mean for a COO?

It means my day has begun. The first thing I try to do is to gather the most relevant information on each topic in order to make the best decision in the shortest time possible.

At the close of this edition, we are a company that operates in 15 countries, each with its own reality, and across multiple time zones, so we are constantly adapting to what we have to face.

What would be the best metaphor to describe a typical work day?

Every day is different. This "annual triple-digit" expansion is truly vibrant. I would say the best representation is a racing car, where attention to detail and coordinated teamwork lead us to the finish line.

What are your main responsibilities in this position?

I am in charge of growing developing, meeting, and exceeding the goals of all areas that are part of the Operations function. I am an orchestra conductor; I love to lead. At the same time, my entire management goes hand in hand with an outstanding work team which includes experts in each area and, notably, an engineering team that is absolutely enviable.

The areas within my scope include Pre and Post Sales Engineering, Delivery with PMO, Customer eXperience, Sales, BDMs with BUs, cross-functionality throughout the organization, Communication, and Marketing.

How do you divide your time among the different work functions?

From my perspective, having a well-organized

agenda and a plan with clearly defined objectives, roles, and responsibilities is essential. This organization helps focus on the short term and daily execution.
Of course, many factors are not accounted for in it, and here is when things can get challenging, and efficiency becomes crucial in order to complete all tasks planned.
In the company, we have calibrated processes and a well-developed practice, supported by the systems. Regular cross-functional meetings and always being open to dialogue and to listen attentively can help you anticipate. Then, you usually dedicate more time to what comes more naturally to you.
That is when an organized agenda puts you on the right track and helps you balance your time with all the activities.

> **“The reality of each of the different countries, with their political and economic situations, is a significant daily external challenge.**

What are the most important challenges you face daily?

The reality of each of the different countries, with their political and economic situations, is a significant daily external challenge.
Internally, I would say that this growth in businesses, countries, and employees makes it very exciting and challenging. Ensuring that teams are well-supported and effectively managed is essential in an environment with such rapid expansion; sometimes, it feels like e a whirlwind. At the same time, and with the help of the Compliance Department, our ISO certifications help us avoid getting overwhelmed because of the rush.

If there were very good news, what would it be?

Continuing to make an impact with high-value projects for society, companies, and individuals, as well as continuing to grow as we are doing in all the countries where we operate.
Continuing to achieve regional recognition from strategic partners, such as manufacturers and customers, is a rewarding indicator of this.
I love winning; I really enjoy it.

Describe a moment of relaxation or play during the workday.

I really enjoy stepping out of the office, grabbing a coffee at a local café in any of the countries where we have a presence, and returning a few minutes later, refreshed, with clear ideas, and having shifted the focus away from immediate tasks.
In Argentina, in particular, I really enjoy the recurring barbecues on the rooftop of one of our office buildings in Buenos Aires, where we share some KPIs with the team, sparking conversations with members from all areas. These are informal gatherings; we are standing, moving from one group to another, quickly connecting and absorbing information. I find it incredibly enriching, and I see it as a very relaxed activity.
I learn a lot from every team member, from their diverse perspectives, different points in their careers, and where each person’s focus lies.
I am proud of the team we have.

How has the role of the COO changed in recent years, especially with the integration of technology?

We operate in the technology industry… so Operations has always been closely linked to systems, processes, and maximizing technological tools to make our work increasingly efficient. I see the COO as an essential leader within the structure, setting the pace for the areas that are in direct contact with the customer.

In other related industries, the Operations role is more focused on solving problems — a little less dynamically — in roles more linked to reporting, logistics, and supply chain.

What role does the COO play in the company's innovation? When is it important not to innovate?
Innovation is something that personally captivates me. Moreover, due to our approach, I am in permanent contact with new technologies and in constant interaction with the leaders of our Solutions and Technical Departments BUs, trying to help achieve the best alliances in the market with a complementary business perspective.

As a company, we have a strategy of in-depth collaboration with manufacturers supported by highly skilled and well-trained engineering, leveraged by multiple international certifications. Being attentive and frequently engaging with the Engineering Department allows us to understand what the next step is or where we should focus our efforts.

As a certain popular saying suggests, you must innovate when you are doing well, because when the results are not favorable, you need to survive. For me, not innovating is not an option.

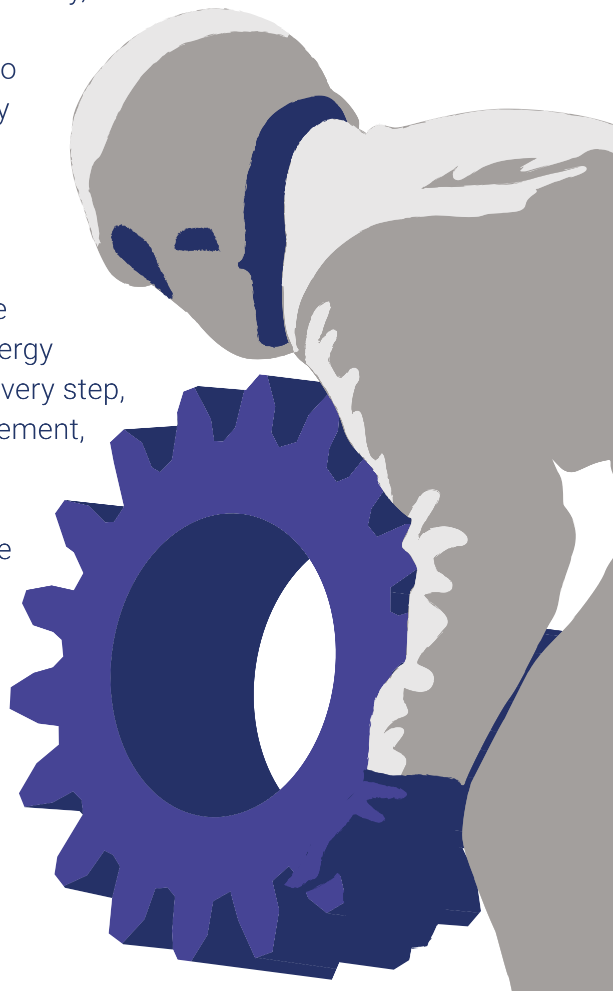
Coffee during the day: yes or no?
Yes, always. I am a big coffee enthusiast and I enjoy that break to recharge and refocus.

What was the most challenging moment in your career as COO?
Something we love at OCP TECH is maintaining that we are an organization with a corporate mindset and a startup heart. Integrating cultures without falling into repetitive patterns and achieving expansion from 4 to 16 countries, exceeding the KPIs set by the CEO, has been a truly spectacular challenge that I will always cherish in my professional journey.

In your view, what is the most important thing a COO must have to be successful?
Passion for what you do, and forming an aligned team that you can learn from and where you have an impact every day. Spreading enthusiasm, being generous with experience, and having the ability to appreciate others' achievements. It is always "together with everyone.".

Do you use generative AI in your daily management? For what purpose?
Some of the solutions we offer have AI as part of their innovation. We must pay close attention to these advancements, since they make a substantial difference in various aspects:
I notice its significant impact, particularly in customer service, in the swift implementation of technological solutions, and the immeasurable efficiency that it brings.

Is there anything else you want to add that I haven't asked you?
I would like to highlight a couple of things that, in my opinion, play a key role in the success of OCP TECH. Firstly, the vision of Leo (Leonardo Scatturice), our CEO, who clearly saw a few years ago the possibility of developing a high value-added integrator to delve into the most important technologies in the market and the impact of the solutions on people. A tenacious and visionary businessman, a great leader who gives us absolute freedom of action, trusting our decisions and allowing us to act. Secondly, an incredible team eager to excel in every aspect. Both the leader and the team are an inexhaustible source of energy that values every step, every achievement, and always strives for more until we successfully reach our goal.



People-centered sustainability

by **Verónica Funes**
HR Manager, OCP TECH

Making correct use of current resources without compromising those of future generations is much closer to daily life than a concept might suggest. It particularly relies on people and their responsible actions.

If we look inside organizations, we might conclude that an organizational culture in line with external proposals and developments in pursuit of sustainability provides coherence and meaning. A strategy is unsustainable if it lacks the support of the values, habits, and behaviors of those implementing it. Therefore, focusing our organizational culture on people, in a Customer-Centric style, involves training collaborators in each of their roles with the skills that will support the strategy.

In this sense, a model that has been particularly useful to me, both at OCP TECH and in other companies, is the 3 H's: Humility, Humanity, Humor.
Let's take a closer look at what behaviors each one promotes.

3 H's to sustain sustainability

Humility

- Being tolerant of different points of view
- Embracing diversity
- Maintaining consistent, open communication between the organization's internal and external spheres
- Encouraging continuous learning
- Being self-reflective
- Acknowledging our mistakes and learn from them
- Expressing gratitude and offering apologies

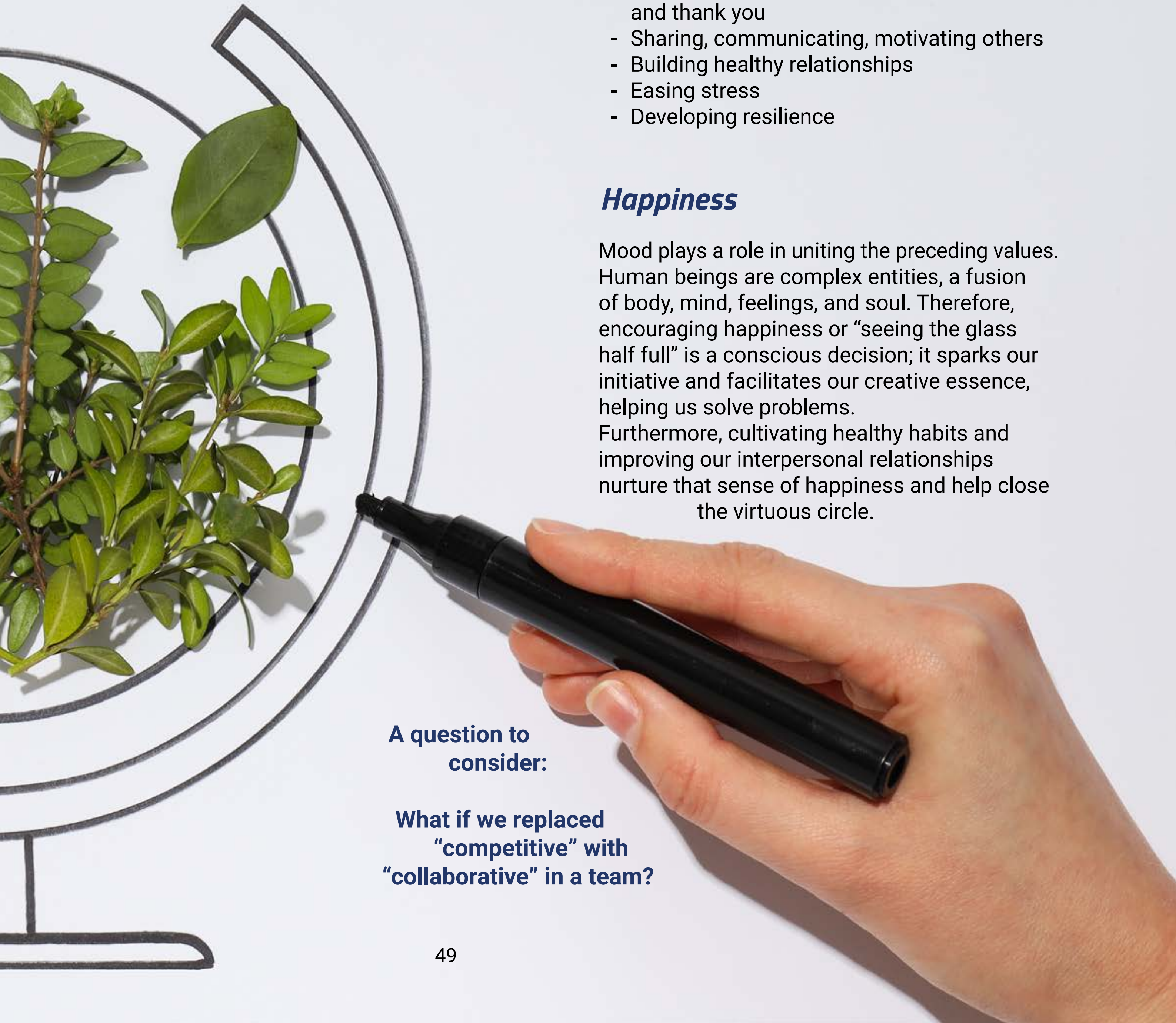
Humanity

The development of technology is generating a flood that sweeps us away, and the difference we can make lies our most human side: generosity, for example. Other skills to develop include:

- Empathy
- Trust
- Work ethics
- Respect to others
- Being close and sensitive to those around us
- Frequently using the magic words: please and thank you
- Sharing, communicating, motivating others
- Building healthy relationships
- Easing stress
- Developing resilience

Happiness

Mood plays a role in uniting the preceding values. Human beings are complex entities, a fusion of body, mind, feelings, and soul. Therefore, encouraging happiness or "seeing the glass half full" is a conscious decision; it sparks our initiative and facilitates our creative essence, helping us solve problems.
Furthermore, cultivating healthy habits and improving our interpersonal relationships nurture that sense of happiness and help close the virtuous circle.



A question to consider:

What if we replaced "competitive" with "collaborative" in a team?

How can we maintain **“humanity”** in the technological age?

In a world where technology continues to amaze us with its advances, and companies constantly seek innovation, Corporate Social Responsibility stands out as a fundamental pillar to reorganize strategies that prioritize the construction of a more sustainable and equitable society.

Corporate culture and human values can make a difference in a world impacted by technology. OCP TECH — a company that seeks to add value to its own organization, to the business of its clients and suppliers, and to the community at large — understands that Corporate Social Responsibility (CSR) is key for individuals and companies to prosper in an increasingly digitalized world. Technology provides a scope of tremendous impact; its magnitude is unprecedented, and its relevance will be sustained in the future. Therefore, the ethics and social skills associated with this discipline become even more significant.

OCP TECH is the first Latin American company to receive Anti-Corruption Certification and holds the Inclusive Company Certification.

Shared vision

What is CSR? Nowadays, in addition to generating profits, companies recognize that their activities impact the quality of life of their employees and their community; therefore, they ensure that their operations are economically, environmentally, and socially sustainable. Regardless of their size, sector, or nationality, they have a shared vision that integrates ethics, transparency, and respect for people, whether they are shareholders, employees, suppliers, clients, or society as a whole.

Organizations related to technology — a tool that has revolutionized our lives and the way of doing business — clearly understand the advantages it has brought, such as quick access to information, facilitated learning, increased productivity, and the breaking down of distance barriers. They also recognize the obstacles to overcome and their role in achieving this. Beyond the qualities of technological products or services, their use leaves an impact on individuals or groups of citizens. The constant use of smartphones, laptops, and other technologies has a detrimental impact on a sedentary human body.

So, **how can we boost physical and mental health?** Today, new trends propose taking CSR towards more comprehensive paths.

Let's get to work

At OCP TECH, they seek to explore innovative approaches that use technology to promote a more active and healthier lifestyle. If you want to maintain longevity, you need to have a body in motion. This process has already begun both in Gaming and in the Metaverse. In the future, senses like taste or smell could be incorporated.

OCP TECH's projects are developed in the public, private, and academic sectors, also addressing intermediate institutions. They collaborate on various projects with the Ministry of Education, the Government of the City of Buenos Aires, the University of Buenos Aires (Universidad de Buenos Aires, UBA), the National Technological University (Universidad Tecnológica Nacional, UTN), the National University of San Martín (Universidad Nacional de San Martín, UNSAM), the Technological Institute of Buenos Aires (Instituto Tecnológico de Buenos Aires, ITBA), the University of Belgrano (Universidad de Belgrano, UB), the Catholic University of Argentina (Universidad Católica Argentina, UCA), as well as with various sports institutions to bring technology closer to sport, among others.

Technology can be an ally in the human journey if used wisely to promote values and general well-being.

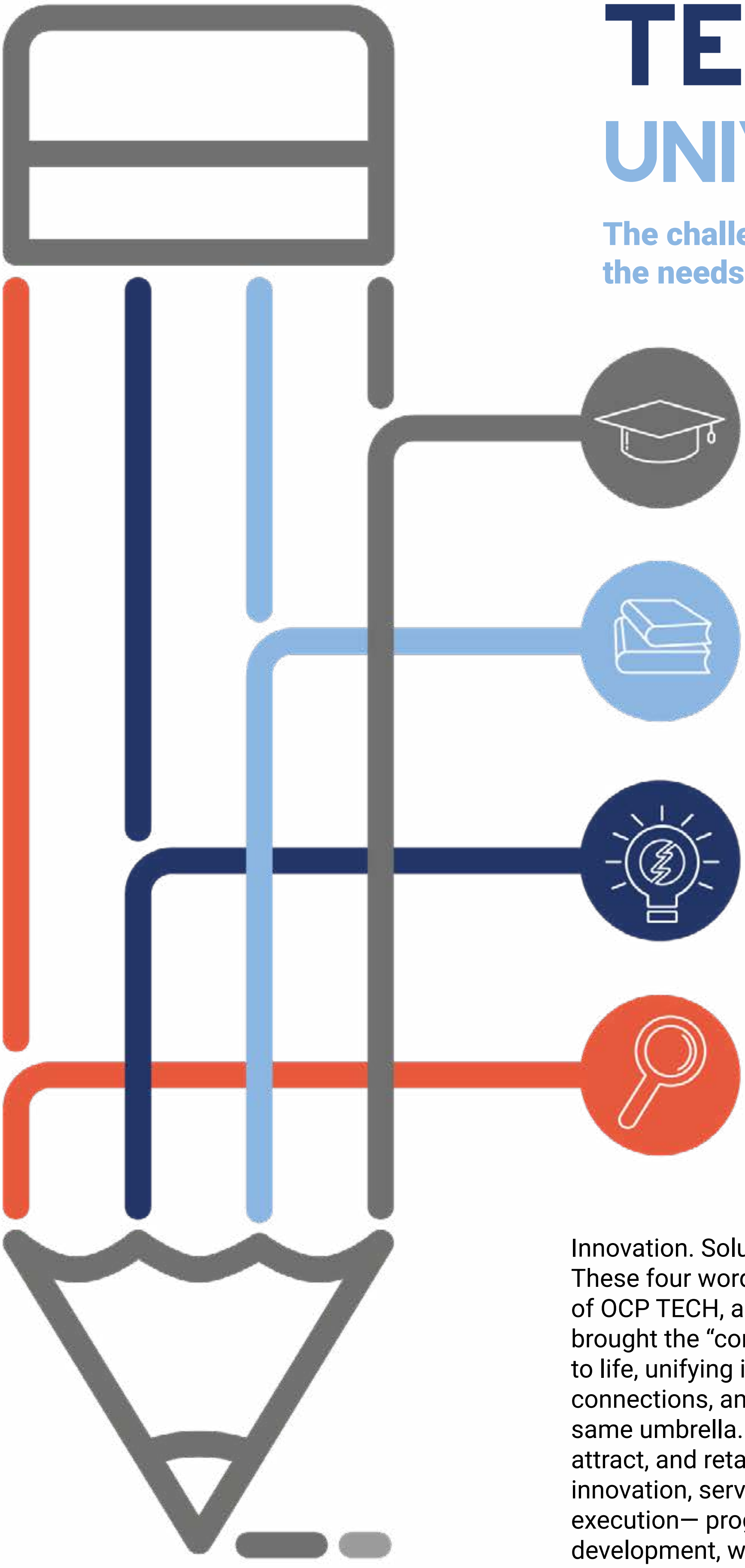
Footprints

by **Karina Basanta**

Challenge
Entering the instance where comfort
spills into the boldness of the experience
Offering ourselves in collaboration
Venturing towards the other, finding them
Proposing the finest version of what is ours
Doing with impact
Positive impact
Precise impact
Sliding and extended impact
If there were a metaphor for understanding,
what would it be?
And what about one for the I-know-how-to-collaborate-with-your-success?
If there were a metaphor for satisfaction,
it would have to be unfolded now
Because the fantasy between our organizations
must be compatible
to be accomplished
with the simplicity of unity

OCP TECH UNIVERSITY

The challenge is to adapt to the needs of the labor market



The future of work poses challenges as well as opportunities. For those who are willing to learn and reinvent themselves, OCP TECH promotes continuous learning, training, and skill development.

Innovation. Solutions. Integration. Engineering. These four words embody the strategic focus of OCP TECH, an organization that successfully brought the “concept” of OCP TECH University to life, unifying internal training, academic connections, and university lectures under the same umbrella. The strategy is to develop, attract, and retain talent so that —through innovation, service integration, and certified execution— progress is made towards development, while balance is achieved in terms of advantages, opportunities, and efficiency. This approach ensures that the best solutions are implemented in a world that is constantly evolving. In this sense, OCP TECH University collaborates in creating a virtuous circle of delivering and receiving knowledge that facilitates learning processes and the accumulation of experience.

The mission and its applications

Through a cross-functional methodology and a dynamic system, the aim is to organize internal and external information, unify the academic and corporate worlds, and offer tools and effective communication in line with the concept.

The structure prioritizes two thematic axes:

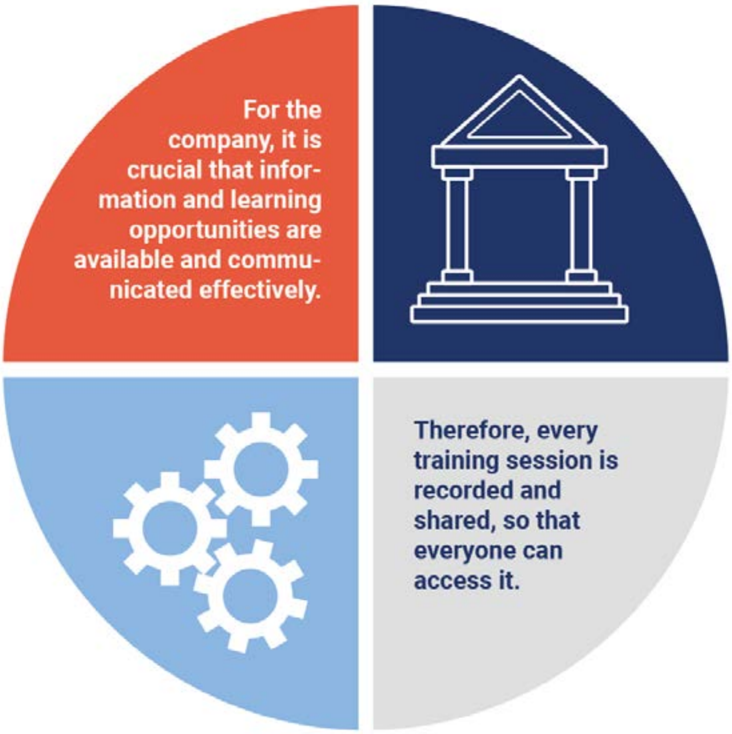
- Training for collaborators through various programs.

- Thematic talks in educational institutions, aiming to present the proposal and provide an insight into technology.

The philosophy of OCP TECH University is to promote a culture of continuous learning among all company profiles. It embraces both young and experienced people, helping them remain open to knowledge and constant updates, adapting to new technologies, methodologies, and skills throughout their careers.

The OCP TECH University training agenda includes topics such as:

- Induction talks.
- Compliance program, including awareness lectures on anti-bribery policy and quality certifications.
- Sales school proposal, led by an interdisciplinary team capable of providing comprehensive, innovative solutions with social impact.
- Lectures on cybersecurity, software development, hybrid cloud infrastructure solutions, and innovation, which drive more efficient, cost-effective, and scalable processes.
- Performance evaluation tools.
- Soft skills program.
- Training for managers, aimed to promote effective personnel selection.
- Talks on commission calculations, with specific tips for managerial level.
- Other topics.



For the company, it is crucial that information and learning opportunities are available and communicated effectively.

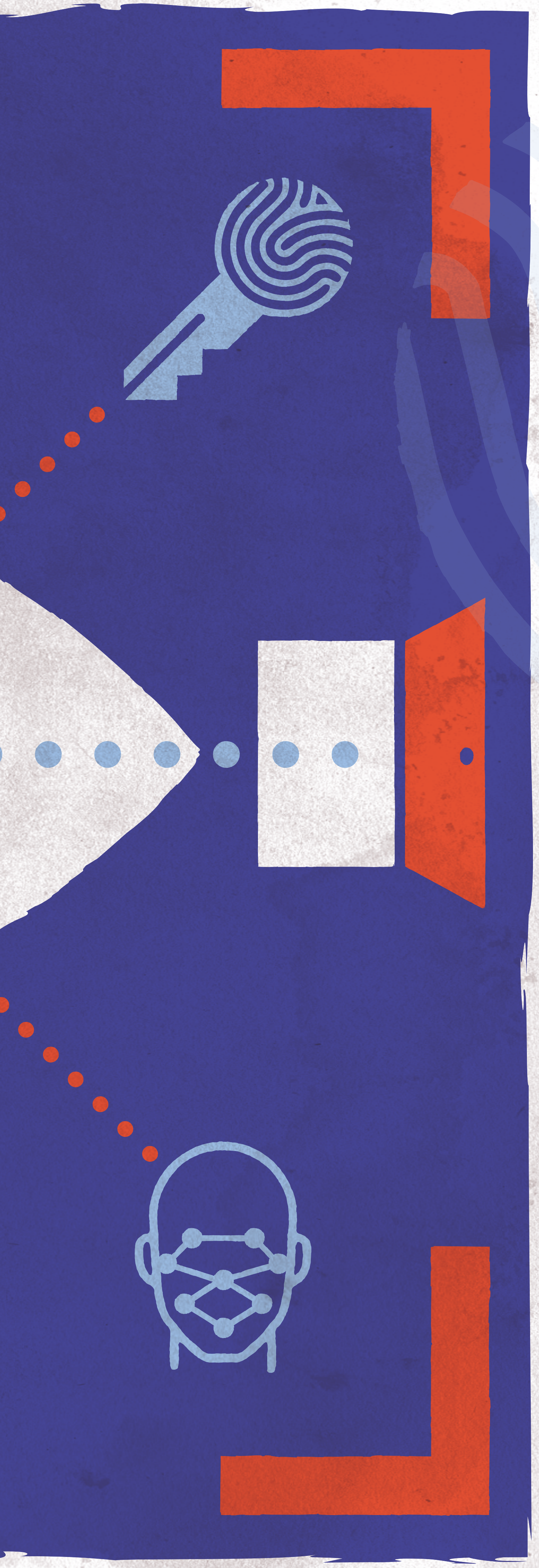
Therefore, every training session is recorded and shared, so that everyone can access it.

The human factor

In addition to theory, training and programs are focused on developing practical skills that are applicable in the work environment, such as leadership, creativity, and other competencies required today in daily management.

Verónica Funes, HR Regional Manager at OCP TECH, says: “Work is changing. In the future, we will need more human potential and critical thinking. The value comes from the human touch.” She also highlights the social responsibility of creating reskilling and upskilling programs to help people stay updated and adapt to changes in the labor market.

In this process, collaboration with educational institutions is essential to bridge the gap between the academic world and the needs of the labor market. Participating in university events, talks, and educational collaborations can help minimize the disparity between formal education and the skills required in the industry.



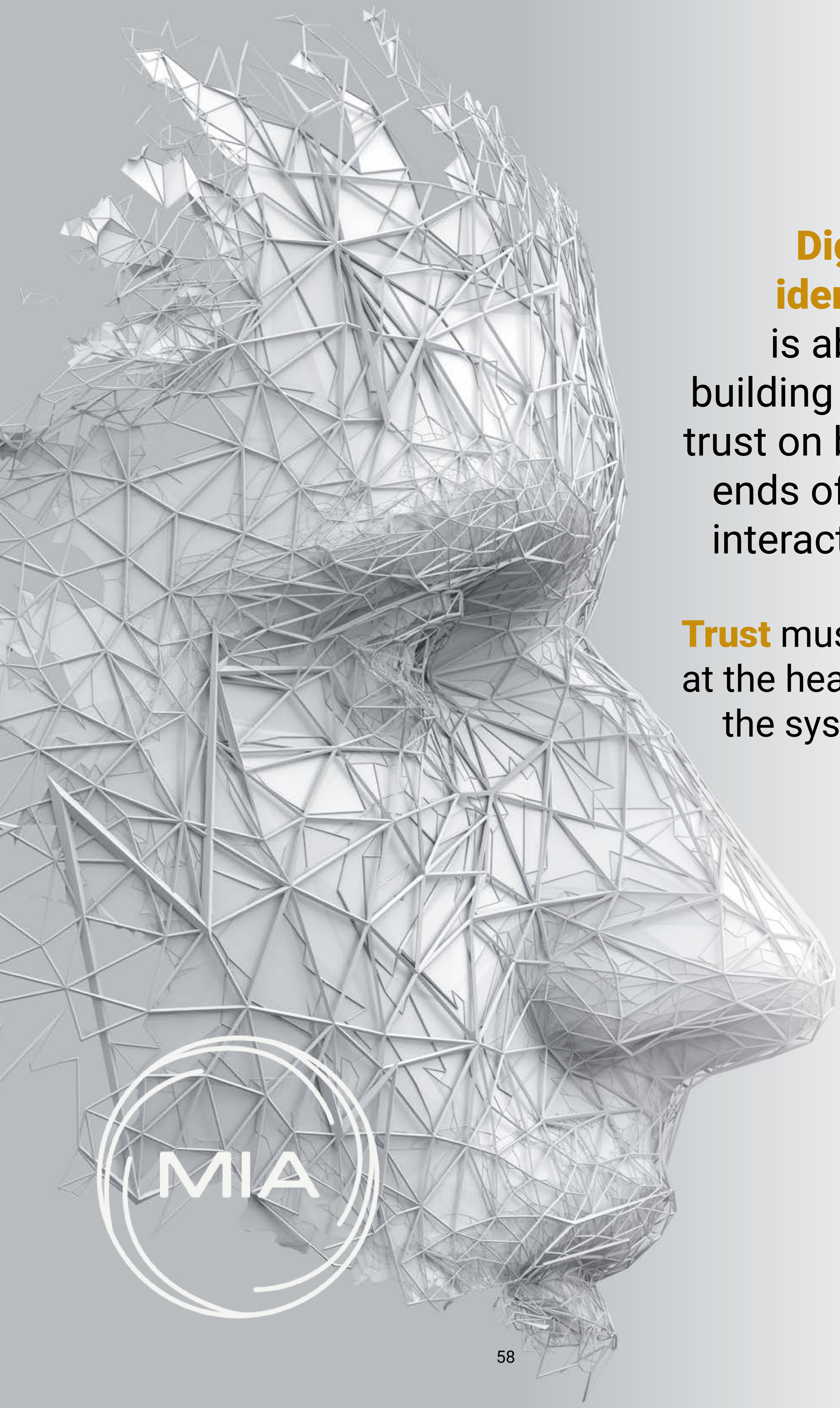
Biometric authentication for secure access

Our biometrics and patterns of behavior identify us.

They are **personal** and unique

Along with well-known authentication systems, such as the use of fingerprint, iris, voice and face recognition, new systems are being implemented, including the way of walking or standing, the veins of the hands, and body smells. Technological advances at the service of authentication for secure access.

Illustration by
Santiago Guerrero



Digital identity is about building that trust on both ends of the interaction.

Trust must be at the heart of the system.

Unique digital identity

by **Gabriel De Simone**
Team Principal MIAid, OCP TECH

We are contributing to shaping a world where individuals and their devices can digitally interact seamlessly with each other and with organizations, fostering trust and eliminating unnecessary friction; a world where people can be easily identified, enabling them to access the services or experiences they want; a world where our digital interactions have evolved into a multifaceted landscape—ranging from PCs and smartphones to smart homes, cars, and mobile devices—and activated by voice, touch, and physical presence.

Some years ago, we entered the era of hyperconnectivity, where digital services integrated into people's daily lives. This has brought us significant benefits as consumers, producers, citizens, and human beings. Digital services have transformed shopping, business, political involvement, healthcare services, and communications. That is why it is essential to establish and safeguard trust in digital interactions—simply, swiftly, and securely.

With current authentication processes, an average user has around 100 login credentials to manage, each with diverse rules for passwords and validation. However, identity fraud is on the rise and has become a more significant issue online than offline.

MIA's goal is to Facilitate and Restore trust in the digital world by simplifying people's lives while also protecting institutions.

The principles of Digital Identity

Today, people pay for their digital interactions with data and privacy. Every day, they are required to provide personal information to access basic digital services.

Often, they don't know where that data is stored, how secure it is, how it will be marketed, and who benefits from it.

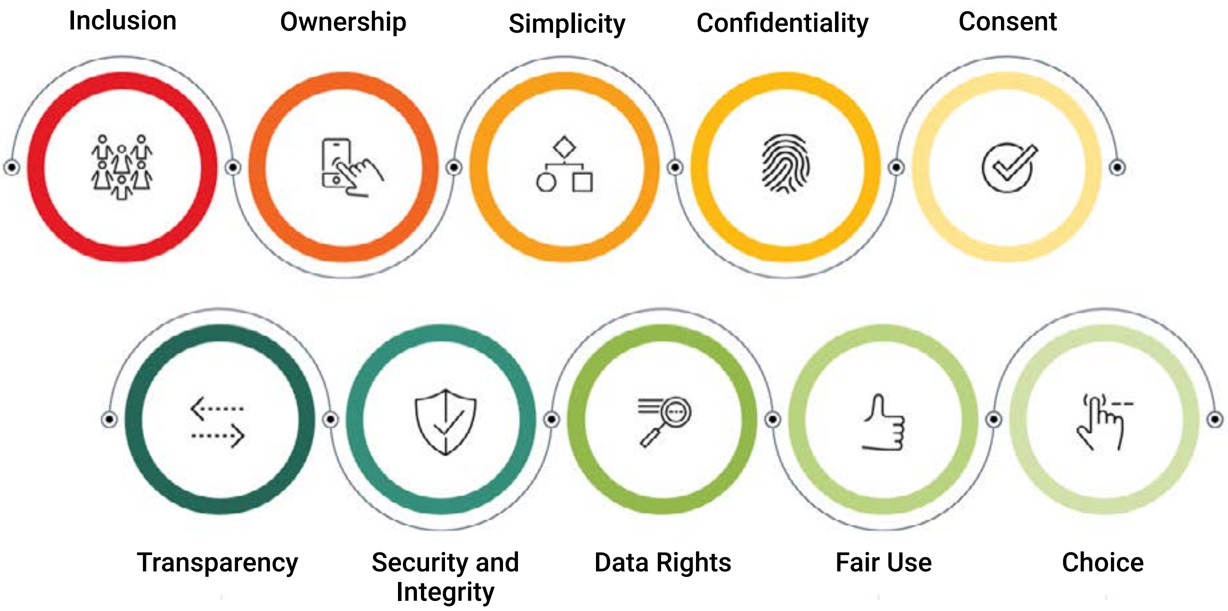
This poses a significant disadvantage for individuals, and particularly for companies, banks, and governments. As individuals are compelled to share their information without control, they only end up exposing details that are later used to gain unauthorized access to private accounts and confidential information.

The current mechanism harms all parties, as it makes it more difficult to trust those making purchases, accessing services, or signing documents. As a result, the entire system becomes more complex and insecure. People are compelled to visit public offices to request documentation, access a benefit, or even schedule a simple appointment. Even online shopping has become increasingly complicated, especially for high-value goods, as the associated risks introduce friction into everyday interactions.

Privacy regulations, such as the General Data Protection Regulation (GDPR) in the European Union, played a crucial role in rebuilding trust and creating a welcoming environment for modern identity infrastructures. However, that is just the beginning, since, ultimately, we are still not certain about "who is on the other side."

The MIA model gives users control and addresses issues related to privacy, ownership, transparency, and security, among others. In essence, individuals own their identity and control their identity data.

Placing the individual at the center of the digital identity ecosystem is essential.
Our guiding principles promote trust and understanding while restoring control over personal data to the individual.



MIA Citizen ID

MIA's Self-Sovereign Identity (SSI) solutions put the resident in control of their own data and make personally identifiable information independently verifiable, eliminating the need for a government agency to store any sensitive data. With SSI, individuals decide how much information they share and with whom they share it, just as they do with their physical wallet and credentials. Organizations that request identification do not retain any personal information, and users have complete control over everything.

For these reasons, several state agencies are looking to SSI to efficiently and securely verify the credentials of residents while conducting transactions online, such as renewing driver's licenses, registering vehicles, and obtaining business licenses.

Control over personal information

With Reusable Digital Identity, individuals can selectively share their credentials based on what is required for that transaction. They can also dictate how that data should be used and revoke data sharing permissions at any time. The government only gets the information it needs when it needs it, while residents maintain control over their personally identifiable information (PII).

Interoperability for better efficiency

The Unique Digital Identity allows greater speed and security. Processing time is substantially reduced, and agencies can quickly work through requests. Moreover, residents benefit from the convenience and service they expect in their digital lives.

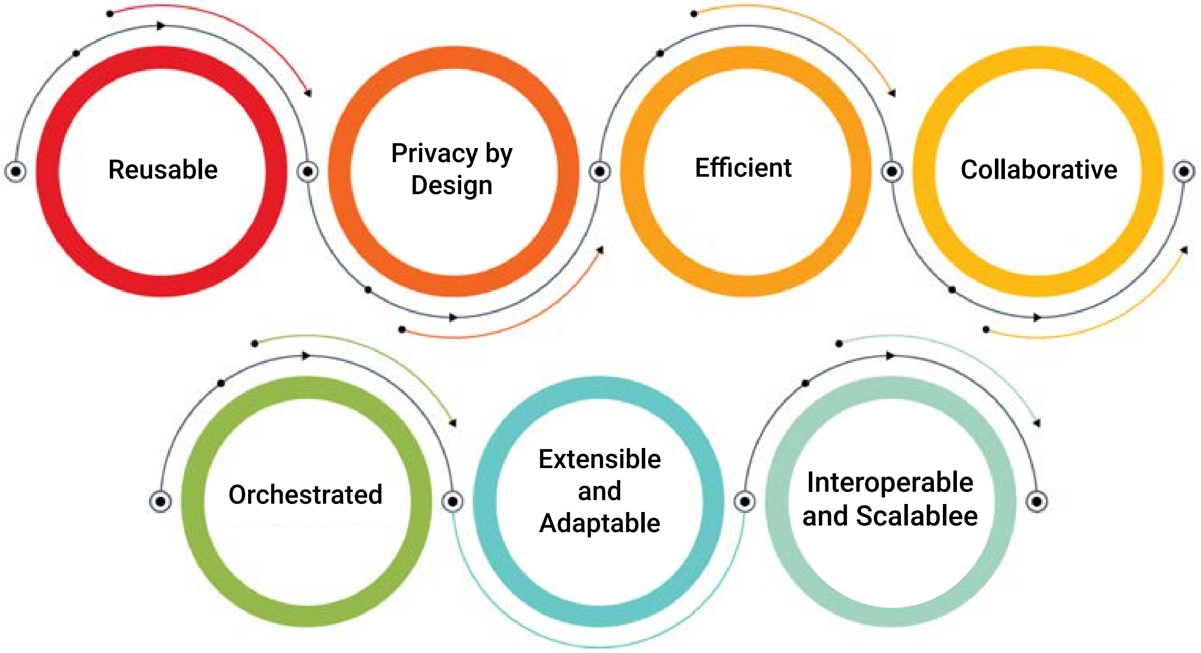
Enhanced Security and Trust Maintaining control of information

MIAid enables governments to issue credentials in a standardized format, such as SSI, using Verifiable Credentials. These credentials are signed by DIDs (Distributed Digital Identifiers) and authenticated through MIA's biometric process. This ensures that the information governance process remains unchanged, meaning that the data stays in the same government repository. The citizen now receives a Verifiable Credential stored in MIA or in any Wallet compliant with the SSI standard, ready to be presented in any private service anywhere in the world.

Now, their information is secure, the citizen has control over it, and their data is protected for any interaction with third parties.

The change in the Interaction model

Other Systems	MIAid
Customized, specialized, and closed systems	Transparent and globally interoperable services
Excessive data sharing without transparency	User-controlled data sharing
Use of static identity data	Use of dynamic and biometric identity data
Hundreds of vulnerable passwords	A reusable digital identity applicable everywhere
An **exclusive** system	An **inclusive** system



Pillars of the MIA model

Interoperability and reusability of digital identity: Eliminates the need for multiple passwords and identity verification procedures. A digital identity enables people to use a single means to authenticate across multiple digital services, including websites, apps, devices, and more.

Privacy by Design: Enables users to protect their data and experience transparency in managing their digital lives.

Efficiency: Being more secure should not be more complex for people. Efficiency helps implement new value-added services, enhance engagement, reduce friction, lower identity costs, improve security, and comply with regulatory requirements.

Collaboration: Both technology and operational stakeholders cooperate to define standards and regulations.

Orchestration: Replaces data aggregation with an orchestrated ecosystem of distributed data.

Extensibility and adaptability: Built around a core that can be fully or partially implemented, adhering to country-specific standards, regulations, and norms.

Interoperability and scalability: Secure interaction is enabled between official data infrastructures and private sector participants, while complying with defined standards in functionality, performance, security, and other regulations specific to local markets.

A Collaborative System fosters trust in an identity transaction.

MIA acts as an accredited digital identity service provider to offer all participants the trust and assistance they need to navigate a complex multi-stakeholder digital environment.

OCP TECH

IMPACT ENGINEERING

NATIONAL POLICE OF COLOMBIA

Executive Summary

Sector: Public.
Country: Colombia.

The Organization: The Colombian National Police force, comprising 165,794 individuals, includes women and men, both uniformed and non-uniformed, across all categories. Its mission as a force lies in maintaining coexistence as a necessary condition for the exercise of public rights and freedoms, ensuring that the inhabitants of Colombia live together in peace, guided by the police code of ethics. By 2030, the goal is to evolve into an organization capable of responding to social changes at both local and global levels, as a result of structural transformations fostering culture and awareness of a responsible future among citizens.

The Police embraces the following as a Big and Audacious Goal:
"Over the first four years, we commit to delivering police services through the institutional unit to address diverse generational and regional behaviors that affect coexistence. This will be achieved through innovative approaches, leveraging technological tools, and optimizing resources."

The Units comprising the National Police include:

- Metropolitan Police and Police Departments
- Directorates and Advisory Offices
- Police Academies
- Specialized Units and Groups
- Police Unit for the Construction of Peace
- Internal Control Office
- Office of International Relations and Cooperation – (ORECI, as per its acronym in Spanish)
- Police Aviation
- International Center for Strategic Studies against Drug Trafficking
- Safe Departments and Municipalities
- General Inspection and Professional Responsibility
- Crime Observatory
- Ameripol Colombia
- National Police Standards Center

The Challenge: Enable access for all police officers in the force to corporate applications from their mobile devices, eliminating the need for passwords and double-factor authentication.

The Solution: ORACLE One Time Password and MIA (Mobile Identity Access) by OCP TECH—a combination of traditional and cutting-edge technologies.

Implementation Status: Completed.

Next Steps: Consolidation of services through platform utilization in 2024.

MOOREA

at the forefront of transformation digital

To delve into this impactful realm for the company, we spoke with Hernán Piñero, VP Sales NOLA, OCP TECH.

Why is this segment of interest to OCP TECH?

Our Moorea platform stands out as a unique solution within its segment, especially for the public sector across the countries in which we operate. It has a significant advantage over other platforms in the market: it is built on open source code, which ensures operational continuity for the customer, regardless of license fee payments. The customer owns the solution and its source code, empowering them to generate their own forms, files, and procedures in the future.

What initiatives are taking place?

Projects are being managed in various organizations at the national and provincial levels in Argentina. In addition, in 2023, the process of positioning the platform in the rest of the region began. We already have projects underway, POC (Proof of Concept) and demos in Colombia, Ecuador, Peru, Panama, Guatemala, and the Dominican Republic.

What is the challenge to overcome?

In Argentina, Moorea has established a name and a recognized presence. Our goal for the rest of the region is to have at least one reference case in each country by the first half of 2024.

How does OCP TECH do it? Why choose OCP TECH for a project of this nature?

Unlike our competitors, OCP TECH’s proposal not only involves the platform and services for the digital transformation or “paperless offices,” but also relies heavily on the customer adoption and training plan led by the CX team. It is a long-term program where, upon completion, the customer learns about and uses their technology, is capable of programming the visual aspect (processes), deploying their own forms, and potentially even performing basic programming using in-house staff, hiring collaborators, or through agreements with universities. Therefore, at OCP TECH we do not just deliver a technological solution, but we help governments become more agile, efficient, transparent, and create quality employment opportunities.

Point by point

One of the sectors that gained great significance within companies in 2023 is the Administration and Finance area, facing major challenges as we enter 2024. In this article, we delve into the key strategic and managerial aspects of these departments at OCP TECH, guided by Fernando Antolín Dulac, Chief Financial Officer of the company.

In technology companies, the sustained market expansion poses challenges such as ensuring a steady supply of inputs or products to meet demand. If these companies are based in Argentina, they must also deal with the restrictive socio-economic context, making it challenging to transfer foreign currency abroad and requiring the development of plans to mitigate the effects of inflation and devaluation of the local currency.

Main challenges during 2023

- Strengthen the Supply Chain area to facilitate the sourcing of materials from both local and international suppliers and improve logistics to enhance the efficient delivery to customers.

- Coordinate International Trade tasks with internal and external areas to enable payments to foreign suppliers from Argentina.

- Optimize month-end close procedures to produce higher-quality management reports.

- Mejorar la atención a proveedores desde el sector de cuentas por pagar.

- Engage in investment activities in local currency to mitigate the impact of peso devaluation in Argentina.

- Double the frequency of salary adjustments to offset the effects of inflation in Argentina.

How were these challenges addressed?

- By streamlining processes across sectors.

- By promoting the use of digital tools, including ERP systems.

- By enhancing leadership capabilities through the skills development of managers in each sector.

- By establishing partnerships with external experts (investment funds, for example).

Did the area experience any growth? How?

- Skilled professionals specializing in functional tasks (taxes, accounting, supply, and management) were hired.
- There was a turnover of personnel without increasing the total payroll for the area.
- Computerization, certification, monitoring, and control procedures for all processes were implemented.

Goals for 2024

- Implement a cloud-based ERP (Enterprise Resource Planning) system to record transactions from all countries and prepare a consolidated FS (Financial Statement) in US dollars.
- Define objectives by sector and conduct performance evaluations.
- Enhance the quality of accounting information for the entire company.
- Provide training for employees in the area to foster their professional development.

> "At OCP TECH we focus on the development of our collaborators, enabling them to fully unleash their potential"

Fernando Antolín Dulac.

OCP TECH

1 The first Argentine company to achieve Anti-Bribery certification

In May 2023, OCP TECH became the first company in Argentina to achieve the ISO 37001:2017 Standard certification in Anti-Bribery Management System (SGAS, as per its initials in Spanish) from TÜV NORD CERT. This certification places the company as part of a select group of pioneering organizations in Latin America that seek to promote a responsible and transparent environment through the implementation of this International Standard. This initiative prioritizes commitment, corporate responsibility, and compliance with the highest international standards in business ethics.

Bribery is one of the most common forms of corruption in the business world. Companies and other types of organizations can and should contribute to prevention through the determined commitment of their leaders to establish a culture of integrity, transparency, honesty, compliance, and the fight against bribery and corruption. For this purpose, there is the Anti-Bribery Certification—one of the requirements most demanded by companies in the region—issued by the Anti-Bribery Management System (SGAS).

This certification is regulated by the **ISO 37.001:2017**: standard, a widely recognized International standard in this field that guides organizations in the establishment, implementation, and maintenance of a management system designed for this purpose, since it offers them a series of measures that they may adopt in a proportional and reasonable manner to prevent, detect, and manage criminal conduct of bribery in compliance with the legislation and with other commitments acquired voluntarily. This standard applies to organizations globally, regardless of their size, activity, sector, or whether they are public, private, or non-profit entities.

Incorporating work processes under Anti-Bribery Management has a positive impact on organizations as it promotes:

- ✓ Demonstration of commitment to integrity and ethics in business practices.
- ✓ Establishment of robust policies and procedures to prevent and mitigate bribery.
- ✓ Reduction of the risk of illegal conduct and protection of the organization's reputation.
- ✓ Building trust among customers, business partners, and stakeholders.
- ✓ Compliance with rigorous standards of transparency and legality.
- ✓ Attraction of new business opportunities based on trust and integrity.
- ✓ Clear commitment to honesty, responsibility, and transparency.
- ✓ Contribution of additional value in terms of reputation and business opportunities.

> “This standard regulates the activity of our entire company and is the most transparent way of doing business with our clients”

Andrés Quinn
COO de OCP TECH

DIGITAL IDENTITY

IS THE PASSWORD DEAD?

New forms of identification are leading to the end of passwords. How can we validate our identity today in a unique, private, and secure way?

The future presents us with opportunities and challenges. In today's digital ecosystem, both organizations and individuals are required to constantly adapt, update, and face a digital landscape that offers enhancements while also posing cyber challenges.

Until recently, the user's journey invariably included a fundamental security measure: the password. It was essential for protecting transactions, assets, and information. According to the instructions, passwords are required to include numbers and characters, both uppercase and lowercase, with a specific number of digits; change them periodically; never store them in a cloud-based file and, certainly, never share them. Furthermore, each application requires a different password. Some companies use a password generator aiming at creating more complex and secure passwords. The keys and passwords model implies constant authentication to prove our identity.

This is when the concept of Unique Digital Identity comes into the scene. It is an effective and secure identification system, in line with the digital transformation embraced by organizations and users, facilitated by fast and efficient connections that use the most advanced technologies in the market.

Every transaction or interaction is processed through identity, and in the near future, passwordless authentication will become natural.

Choosing the new path

The time for passwordless authentication has not only arrived but also enhances security and ensures a better customer experience.

Passwordless authentication methods are diverse.

One example is biometric authentication, which verifies a user's identity using physical or behavioral characteristics. Verification can be done through voice or facial recognition, or through fingerprint or iris scanning. Biometrics are increasingly being used in applications. Unlike passwords, biometric data cannot be forgotten or shared and is more difficult to copy or steal.

The Single-Sign-On (SSO) method allows the user to securely log in to third-party applications using a single set of credentials. This is done by logging in, for example, through services like Google, Microsoft, or Facebook. SSO seeks to streamline the user's experience on the Internet by fully simplifying login processes.

Possession Factors, on the other hand, grant access to users through a mobile device or something they possess, such as a specific identification. One-time access codes (OTP) are received via email or SMS and allow users to log in to the system automatically by responding to notifications or entering the codes.

Magic Links are another form of passwordless authentication. It is achieved by sending a unique URL to the user's email, allowing them to log in to the application or account. For security reasons, they are time-limited and unique, meaning they are not valid after a certain time.

Embracing change

Every year, researchers analyze what the most common passwords are, and find that, despite the increasing awareness of cybersecurity, these passwords are consistently used. Users continue to create weak passwords to protect their accounts and data. Additionally, passwords are the most common target of attacks. Cybercriminals use different techniques, such as phishing and brute force, to obtain passwords, allowing them to also gain access to sensitive data belonging to individuals and companies.

Today, passwordless authentication methods can enhance the user experience while optimizing costs, reducing data breaches, and increasing productivity for organizations' workforces.

The challenge for implementing these methods begins with embracing the change and evaluating the best solutions offered by passwordless authentication technology, considering its features and security.

MIA Unique Digital Identity

These are some of the most relevant features of the OCP TECH platform, which ensures a simple and secure passwordless authentication process:

- It is Omnichannel and interoperable: it complies with international standards in terms of data processing and security.

- It offers a channel- and device-independent interaction model, with end-to-end FIDO certification.

- Transactions are authenticated through multiple biometric factors chosen by the user. This eliminates the need for usernames and passwords, as well as traditional second-factor models, such as email or phone number validation. Additionally, the risk of fraud and friction is reduced, thus the flow or experience is not disrupted, and there is no need for additional downloads in other applications or performing complex tasks.

- The more it is used, the stronger it becomes, unlike the username and password model, which the more it is used, the weaker it becomes, because it is more exposed.

- It ensures privacy since the user does not need to expose more information than necessary.

- The information is immutable and cannot be tampered, the data is sovereign, and a specific algorithm is used to make the experience simple and secure.

- In Argentina, MIA is integrated with the National Registry of Persons, with the Nosis application, and with the Federal Administration of Public Revenues.

2 Questions

Two leaders in the technology industry share their insights on how technology contributes to enhancing the performance of an organization.

Andrés López

ICT Secretary, Government of Antioquia

How does technology impact the development of an organization?

Technology contributes by boosting operational efficiency, streamlining internal communication and collaboration, enabling market reach, enhancing the customer experience, and facilitating data analysis for informed decision-making. Key points to consider nowadays include:
Cybersecurity: implementing security measures such as firewalls, antivirus, and endpoint detection and response (EDR) systems, while educating users on best practices and promoting awareness of cybercriminals techniques.
Technology Infrastructure: striving for robustness through servers, networks, cloud storage, and other essential components to support seamless business operations.
Data: given its importance and value, it is essential to implement appropriate policies for secure data handling, encryption of sensitive information, and regular backups to prevent potential loss or damage.
Digital Identity: proper management involves ensuring that only authorized individuals access confidential systems and data through advanced authentication methods.
Data Analysis: effective management involves collecting substantial data volumes, utilizing advanced analytical tools such as AI or machine learning, as well as ensuring privacy and regulatory compliance when handling them.

What is your perspective on Industry 4.0 technologies and their social impact?

Artificial Intelligence, the Internet of Things, and Automation have significant potential to transform society and boost efficiency across various industrial sectors. They can enhance productivity, reduce costs, and improve people's quality of life by facilitating daily tasks and enabling greater connectivity. In addition, these technologies can create new employment opportunities and economic possibilities. However, it is important to weigh their potential social impact. Factors such as job displacement due to automation should be taken into consideration, especially how it might affect certain segments of the population. Privacy and data security, among others, should be considered as well.

Santiago Ezequiel Edreira

Corporate Manager, IT Services Management, Arcor Group

What benefits does technology bring to an organization?

In general terms, technology provides key benefits that drive growth and efficiency. It brings agility, flexibility, and adaptability to face a changing business landscape, enhances the decision-making process, and serves as the distinctive factor to undergo digital transformation. Today, every aspect of an organization is impacted and/or leveraged by technology. There are no longer business processes on the one hand and technological processes on the other hand: every business process is accompanied by technological development, and every technological process serves a business purpose. As an example, I can mention collaboration solutions like Cisco Webex, playing a crucial role in improving communication and efficiency within the organization.

What is your perspective on technologies and their social impact?

When used appropriately, technology has the potential to simplify people's lives and enhance the integration of businesses with their environments; however, it can also damage an ecosystem. Therefore, responsible use of technology is crucial, and clear regulatory frameworks are essential.

Future and Present of **Smart Cities**

Smart cities are those in which information and communications technologies (ICT) are applied to establish the infrastructure that ensures or facilitates their operation. Sustainable development, improved quality of life, and greater effectiveness and efficiency in the use of available resources are some of the incredible benefits that smart cities bring to all citizens.

by **Freddy Macho**
Chairman of the Cybersecurity Research Center for IoT -IIot
Chairman of the IoT Committee of the Cybersecurity Laboratory (OAS)
Regional Coordinator of the Industrial Cybersecurity Center (CCI) of Spain
Expert Researcher ICS – IoT – IIoT (Global Foundation for Cyber Studies and Research)
Chairman of the IoT Security Institute (IoTSI), Chapter Chile
Cybersecurity Advisor – Board of Directors, Holding Company

Responding to the challenge of a growing population

A trend that seems unstoppable is the blurring of the boundaries between cyberspace and the physical world. An expression of this integration is the Internet of Things (IoT) and the proliferation of network-connected devices, extending far beyond smartphones or smart home appliances. The Internet of Things is a new paradigm shift in the realm of information technology (IT), where things have digital identities, functionalities enhanced with artificial intelligence (AI), and can be located, tracked, monitored, controlled, and automated. The acceleration towards digitalization and remote work has driven the exponential growth of hyper-convergence.

The world population is growing steadily. In fact, according to a United Nations report, approximately 83 million people are added every year. The current number of inhabitants is estimated to be around 7.3 billion people and to reach 9.7 billion by the year 2050. Furthermore, the Department of Economic and Social Affairs of the United Nations has launched a document forecasting that 68% of the population will live in urban areas by 2050. This poses a significant challenge to deliver efficient services for a vast number of inhabitants in densely populated urban areas.

In light of this reality, it is crucial to effectively address concepts such as energy efficiency, sustainable development and environmental protection, reduction of CO2 emissions sent into the atmosphere, decarbonization, progressive elimination of fossil fuel consumption, and control of water demand consumption, among other points. This will ensure an adequate standard of living for the residents of future urban areas worldwide.

When referring to a city as “smart”, we are emphasizing its ability of developing a solid strategic planning process that, based on the needs and opportunities of the area, enables the city to set priorities and be flexible enough to adapt to changes associated with the urban overpopulation and the powerful indicators of climate change.

On the other hand, each city deals with their own problems and growth rate. The positive and negative consequences of population growth have different levels of impact. Therefore, the strategy to prepare the city for the future, transforming it into a smart city, is unique to the area and its community. Working towards achieving a smart city involves the collaboration of the public and private sectors, where the entire community should be and feel part of the transformation: citizens, organizations, companies, the government, research centers, and universities, among others, all seamlessly operating in harmony as a natural ecosystem.

Within the spectrum of areas involved in the challenge of shaping smart cities, at least the following should be considered:.

- Enabling technologies
- Mobility
- Life and inclusion
- Infrastructure and buildings
- Cybersecurity and public security
- Economy
- Education
- Energy
- The environment and climate change
- Finance
- Fire and emergency response
- Governance
- Health
- Housing
- Population and social conditions
- Recreation
- Safety
- Solid waste
- Sport and culture
- Telecommunications
- Urban planning
- Transport
- Urban/local agriculture and food security
- Sewage
- Water
- Post-pandemic

The deployment of IoT raises numerous cybersecurity issues stemming from the intrinsic nature of smart objects. One example is the adoption of lightweight cryptographic algorithms, in terms of processing and memory requirements, and another one is the use of standard protocols, for example, the need to minimize the amount of data exposed in the exchange between nodes. The integration of the physical world into the fabric of the Web imposes advanced cybersecurity requirements that must be met to ensure strict control over IoT service interaction.

Smart Cities and Cybersecurity

Smart cities improve the quality of life of citizens in terms of energy and water usage, healthcare, environmental impact, transportation needs, public security needs—encompassing both physical (traditional crime) and logical (cybercrime) security—and many other essential city services. Recent advances in hardware and software have driven the rapid growth and implementation of ubiquitous connectivity between the physical and cyber components of a city, particularly with the advent of IoT devices and the deployment of 5G technologies. However, this connectivity also opens numerous doors for cybercriminals to exploit vulnerabilities in cybersecurity, so users must be aware of them in order to implement effective mitigation strategies.

A comprehensive and modern look at smart cities cannot leave behind concepts that are so critical today such as the environment, sustainability, and security. It is not just about enhancing technology or improving service efficiency for city residents; we must ensure that these are provided with environmental responsibility, while protecting both human rights and cybersecurity of citizens.

Opportunities for cybercriminals

In this maelstrom of technologies applied to enhance urban life, undoubtedly the interaction among different stakeholders and the exchange of data are relevant elements for operating these technologies and conducting these activities or processes. In this context, cybercriminals can find some of these opportunities:

- Inadequate or non-existent cybersecurity, both at a general and individual level. The security level of a system is determined by its most insecure component.

- Technology providers that make cybersecurity research difficult or impossible.

- Excessive complexity of systems and platforms, making it more challenging to detect and stop a cyberattack.

- Lack of security testing on these systems, platforms, and technologies.

- Legacy systems with low security, including outdated platforms, software, and technologies where implementing encryption systems is impossible.

- Vulnerability to DoS (denial of service) attacks, involving multiple attacks targeted at the same point with the aim of rendering it inoperative. Attacks could even originate from the city's own connected objects, or at least from those with poor security.

- Risks derived from the inadequate handling by the Administration of the challenges posed by connected cities.

- Inadequate or absence of emergency plans against cyberattacks and lack of incident response teams.

Current cybersecurity challenges:

- Most cities around the world are implementing new technologies without first conducting cybersecurity tests. Basic security practices are being overlooked when implementing new technologies.

- Most technologies are wireless, which poses a significant risk of being hacked if proper encryption controls are not in place.

- Most cities do not have CERT/CSIRT to coordinate responses to cybersecurity incidents.

- Cities often use vulnerable technologies because manufacturers release security patches too late or these are not applied.

- Cities find it challenging to stop using outdated and vulnerable systems. These add complexity and increase the attack surface.

- Cities do not have emergency plans for cyberattacks, so they are not prepared to face them.

- Cities dependency on technology can be exploited by cybercriminals who attack the pillars of cybersecurity: confidentiality, integrity, and availability.

Recommendations

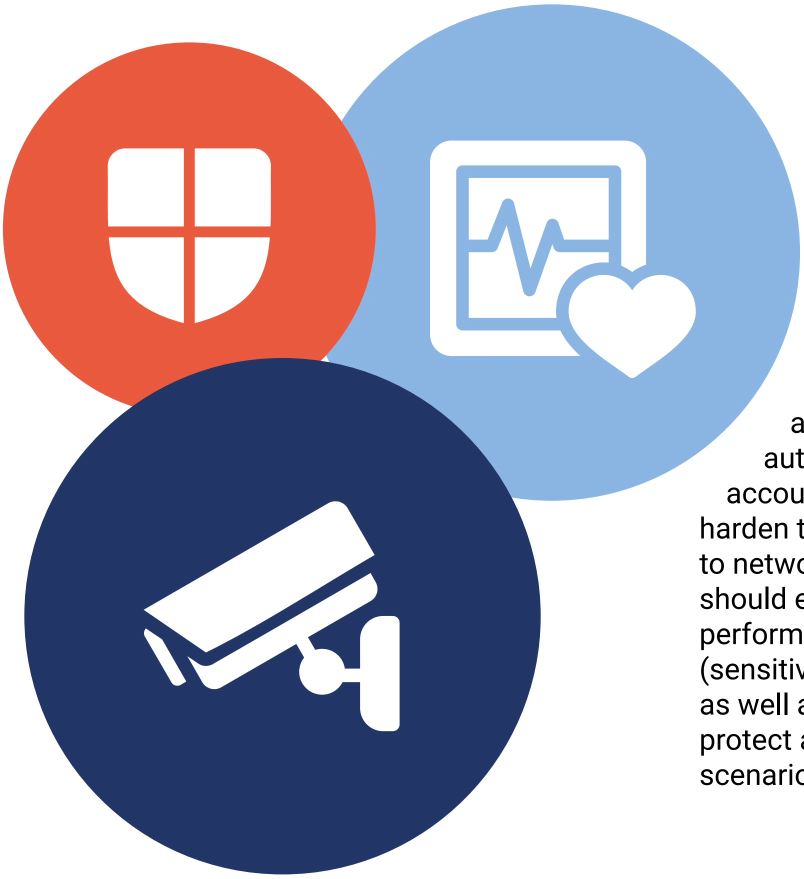
Communities should ensure that any "smart" or connected features to be integrated into new infrastructure are secure by design and include secure connectivity with any existing legacy systems. Additionally, they should be aware that legacy infrastructure may require redesigning to safely implement smart city systems. Security planning should focus on building resilience through a defense-in-depth strategy, addressing both physical and cyber risks. This includes the converged cyber-physical environment introduced by IoT and Industrial IoT (IIoT) systems.

Cybersecurity Best Practices for Smart Cities

Integrating public services into a connected environment can increase the efficiency and resilience of the infrastructure that supports daily life in our communities. However, communities aspiring to become smart cities should carefully assess and mitigate cybersecurity risks associated with this integration. Smart cities are attractive targets for malicious cyberattacks because of:

- The data being collected, transmitted, stored, and processed, which can include significant amounts of sensitive information from governments, businesses, and private citizens.

- The complex artificial intelligence-powered software systems, which may have vulnerabilities, that smart cities sometimes use to integrate this data.



Apply the principle of least privilege

The organizations responsible for implementing smart city technology should apply the principle of least privilege across their network environments. As defined by the US National Institute of Standards and Technology (NIST), this principle states that “A security architecture should be designed so that each entity is granted the minimum system resources and authorizations to perform their tasks. Administrators should review default and existing configurations along with hardening guidelines from vendors to ensure that hardware and software are only allowed to access the systems and data needed to perform their functions.

Enforce multi-factor authentication

The organizations responsible for implementing smart city technology should secure remote access applications and enforce multifactor authentication (MFA) on local and remote accounts and devices, where possible, to harden the infrastructure that enables access to networks and systems. Additionally, they should explicitly require MFA where users perform privileged actions or access important (sensitive or high-availability) data repositories, as well as review configuration policies to protect against “fail open” and re-enrollment scenarios.

Adopt a zero-trust architecture

Implementing zero-trust network design principles will create a more secure network environment that requires authentication and authorization for every new connection with a layered, defense-in-depth security approach. Zero trust also enables greater visibility into network activity, trend identification through analytics, problem resolution through automation and orchestration, and more efficient network security governance.

Manage changes to internal architecture risks

The organizations responsible for implementing smart city technology must understand their environment and carefully manage communications between subnetworks, including newly interconnected subnetworks that link infrastructure systems. Network administrators must be aware of the evolution of their network architecture and the staff responsible for the security of the integrated whole and each individual segment. Administrators should identify, group, and isolate critical business systems and apply appropriate network security controls and monitoring systems to reduce the impact of a compromise across the community.

Securely manage smart city assets

It involves protecting smart city assets against theft and unauthorized physical changes, as well as considering the implementation of physical and logical security controls to protect sensors and monitors against tampering, theft, vandalism, and environmental threats.

Patch systems and applications in a timely manner

Where possible, enable automatic patching processes for all software and hardware devices that include authenticity and integrity validation. Leverage threat intelligence to identify active threats and ensure exposed systems and infrastructure are protected. Secure software assets through an asset management program that includes a product lifecycle process. This process should include planning replacements for components and software approaching or past end-of-life, as manufacturers or developers may stop releasing patches.

Review legal, security, and privacy risks associated with deployments

Implement processes that continually assess and manage the legal and privacy risks associated with deployed solutions.

Proactive Supply Chain Risk Management

All organizations responsible for implementing smart city technology must proactively manage ICT supply chain risk for any new technology, including hardware or software supporting the implementation of smart city systems or service providers supporting the implementation and operations. Organizations should only use trusted ICT vendors and components. The ICT supply chain risk management process should include participation from all levels of the organization and be fully supported by program leaders implementing smart city systems.

Software Supply Chain

The organizations responsible for implementing smart city technology should establish security requirements or controls for software vendors and ensure that potential vendors use a software development lifecycle that incorporates secure development practices, maintains an active vulnerability identification and disclosure process, and enables patch management. Product vendors should also assume some of the risk associated with their products and develop smart city technology compliant with security-by-design and security-by-default principles while ensuring active maintenance of the products they offer.

Hardware and IoT Device Supply Chain

The organizations responsible for implementing smart city technology must determine whether the IoT devices and hardware that will enable “smart” functionality will require support from external or third-party services. They must conduct thorough research into how parts are sourced and assembled to create products. They should also determine how devices store and share data, as well as how they protect data at rest, in transit, and in use. Organizations should maintain a risk register that identifies both their own and their vendors’ dependency on cloud computing support, externally sourced components, and similar dependencies.

Managed Service Providers and Cloud Service Providers

Organizations should establish clear security requirements for managed service providers and other vendors that support smart city technology implementation and operations. Additionally, they should consider the risks of using third-party vendors in their overall risk management planning and ensure that organizational security standards are included in contractual agreements with third parties. Similarly, organizations should carefully review cloud service agreements, including data security provisions and shared responsibility models.

Operational Resilience

The organizations responsible for implementing smart city technology must develop, assess, and maintain contingencies for manual operations of all critical infrastructure functions and train staff accordingly. Those contingencies should include plans for disconnecting infrastructure systems from one another or from the public Internet to operate autonomously. In the event of a compromise, organizations should be prepared to isolate affected systems and operate other infrastructure with as little disruption as possible.

Backup systems and data

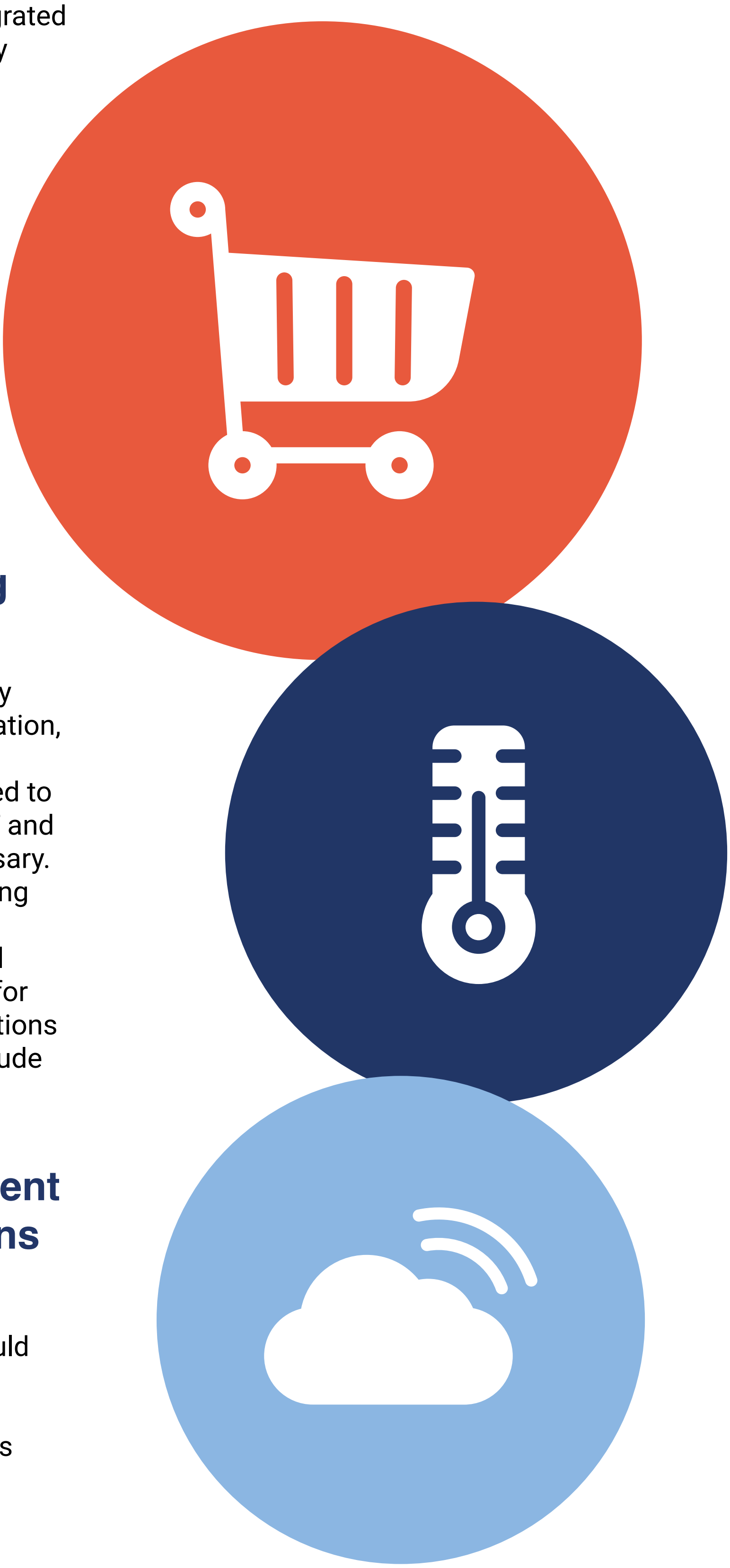
The organizations responsible for implementing smart city technology must create, maintain, and test backups, both for IT system records and for manual operational capabilities for the physical systems integrated in a smart city network. They must identify how and where data will be collected, processed, stored, and transmitted, and ensure that every node in that data lifecycle is protected. System administrators should store IT backups separately and isolate them to inhibit the spread of ransomware. Many ransomware variants attempt to find and encrypt or delete accessible backups. Isolating backups enables systems/data to be restored to their previous state in the event of such an attack.

Conduct workforce training

Although the implementation of smart city technology may include extensive automation, employees responsible for managing infrastructure operations must be prepared to isolate compromised IT systems from OT and manually operate core functions if necessary. Organizations should train new and existing employees on integrated and automated operations, as well as on isolated, manual backup procedures, including processes for restoring service after a restart. Organizations should update training periodically to include new technologies and components.

Develop and exercise incident response and recovery plans

Incident response and recovery plans should establish roles and responsibilities for all stakeholders, including executive leaders, technical leaders, and procurement officers from inside and outside the smart city implementation team. The organizations responsible for implementing smart city technology should maintain up-to-date and accessible hard copies of these plans for first responders in the event the network becomes inaccessible (for example, due to a ransomware attack). Organizations must exercise their plans annually and coordinate internally to ensure continuity of operations.



General Production
Basanta Contenidos

Editorial Director
Karina Basanta

Art Director
Nicolás Cuadros

Coordinators
Marta Azzani
Emiliano Martínez

Audiovisual Production
Salpufilms

Collaborated on this edition
Silvia Montenegro

Photography and Illustration
Basanta Contenidos
Santiago Guerrero
Freepik

Translation
María Gimena González Marino

Acknowledgements
Claudia Menkarsky
Freddy Macho
Pablo Marrone
Eric Balderrama

basantacontenidos.com
basanta@basantacontenidos.com
@basantacontenidos
+54 911 5014-4510 / 5260-8723

Printed by: FP Impresora
Antonio Beruti 1560, Florida Oeste,
Buenos Aires
Tel: 11-4760-2300
www.fpimpresora.com.ar

The editor is not responsible for the contents of the advertisements and articles, and it is solely the responsibility of companies and/or authors. The Publisher reserves the right to reject requests for advertisements. Reproduction, in whole or in part, of any article, section, or graphic material published in this magazine is prohibited.

OCP TECH

IMPACT ENGINEERING

@somosOCPTECH ocp.tech /ocp-tech @OCPTECH