SECURING OUR DIGITAL IDENTITY

BDO

CONTENTS

THE 5 FUNCTIONS OF CYBERSECURITY

Your security strategy should consider each of them.

IDENTIFY
Manage cybersecurity risks that apply to the organization and business continuity, including systems, processes, people, assets, and information.

PROTECT
Ensure and guarantee the delivery of critical infrastructure services for the organization, considering limiting or containing the impact of a potential cybersecurity event.

DETECT
Identify the occurrence of a cybersecurity event, allowing for timely discovery.

RESPOND
Take appropriate measures in response to a detected cybersecurity incident, including the ability to contain its potential impact.

RECOVER
Maintain resilience, contingency, and capability or service restoration plans for those affected by a cybersecurity incident; recovery is aimed at returning to the organization's normal operations.

RAISING AWARENESS

Small acts of awareness have a significant impact on security for everyone.

WORKPLACE
Keep your desk free of papers containing sensitive information. Lock your workstation when you step away.

EXTERNAL STORAGE DEVICES
Do not connect untrusted USB devices. Encrypt sensitive information transported on removable devices.

INFORMATION LEAKAGE
Shred all sensitive paper-based information. Do not provide sensitive information if you don't know the recipient.

INFORMATION PROTECTION
Backup all sensitive information stored solely on personal devices.

USE OF PERSONAL AND/OR PUBLIC EQUIPMENT
Avoid handling corporate information on public computers. Do not download files on non-corporate devices sent from work emails.

PASSWORDS
Do not share or disclose passwords. Use complex passwords mixing numeric, alphanumeric, and special characters.

EMAIL
Never send personal data, passwords, or confidential information via email. Use the corporate email address for internal communication.

BROWSING
Do not access untrusted websites. Do not click on suspicious links; type the address into the browser's address bar.

"The digitization of processes brings numerous advantages in the business ecosystem: speed, efficiency, lower costs, but it also puts us on the radar of cybercriminals who evolve and perfect their methods of action."

FABIÁN DESCALZO
Partner in Technology Governance and Cybersecurity

FAMILY ENVIRONMENT CARE

Cybersecurity is not confined solely to the workplace.
Our lives alternate between social, family, and work-related activities.
Here are some recommendations to keep in mind in the family environment.

- Be cautious when receiving an email with a subject, attachment, or hyperlink related to COVID-19.
- Do not share any personal information via email, social media, or text messages with individuals outside your immediate family/ close friends circle.
- Verify the authenticity of social media and SMS messages related to COVID-19.
- Do not respond to any requests to share personal information.
- Exercise caution not to click on suspected malicious links or attachments. There is a significant amount of 'fake news' circulating about the COVID-19 virus.
- Review and configure privacy settings available on each of the social media platforms you use.
- Seek up-to-date information from legitimate sources, such as government websites. Be cautious when installing mobile applications related to COVID-19.
- Whenever possible, it is recommended to limit access by individuals who can see what you are doing.
- Beware of malicious applications, such as 'coronatracker,' which can compromise your mobile device.
- Analyze the information you decide to post, as once something is posted, you lose control over what others do with that material.
- Use your company device when working from home.

CARE IN REMOTE WORK

The future of work transformation today is hybrid, combining in-person and remote work. Here are some security considerations regarding telecommuting:

- If possible, use company-provided equipment. Avoid using personal devices.
- Connect through a Virtual Private Network (VPN). Avoid using public or third-party Wi-Fi networks.
- Exercise even greater caution against phishing. Do not click on links in emails of questionable origin or download attached content from such emails.
- Access only websites that use HTTPS, which provide a secure connection.
- Ensure that the passwords protecting your accounts are strong, unique, and known only to you.
- Keep containers with liquids away from the devices you use.
- Do not store company data on non-business devices when working from home.
- Use your company-provided device when working from home.
- Keep screens clear of post-it notes or papers with business information.
- Do not use personal email for work-related communication.
- Do not use unauthorized programs for corporate data exchange.
- Do not lend your notebook or mobile devices used for work to your children to prevent data deletion or loss.
- Turn off your notebook when not in use.
- Avoid connecting low-quality peripherals.
- Keep the notebook away from hot areas and windows.
- Plug the charger into secure outlets, without adapters or loose connections.

CYBERSECURITY CONTROL SYSTEM

Quick steps you can take now to protect your cybersecurity control system.

PUT SOMEONE IN CHARGE

Appoint one or more individuals to lead your control system cybersecurity efforts.

KNOW WHAT YOU HAVE

Document what types of computer and control system assets you have, how each asset is used, and determine the most critical assets. Verify and remove unauthorized assets.

ESTABLISH CYBERSECURITY RELATIONSHIPS

Join industry-specific cybersecurity communities and build relationships with vendors and integrators who can assist with recommended cybersecurity practices.

CHANGE DEFAULT PASSWORDS

Check your assets for default passwords and change any you find to new, hard-to-guess passwords. Do not leave passwords in plain sight.

PROTECT ASSETS FROM TAMPERING

Physically secure critical assets and keep control system asset keys, such as programmable logic controllers (PLCs) and security systems, in the "Run" position at all times unless actively programming.

AWARENESS AND TRAINING

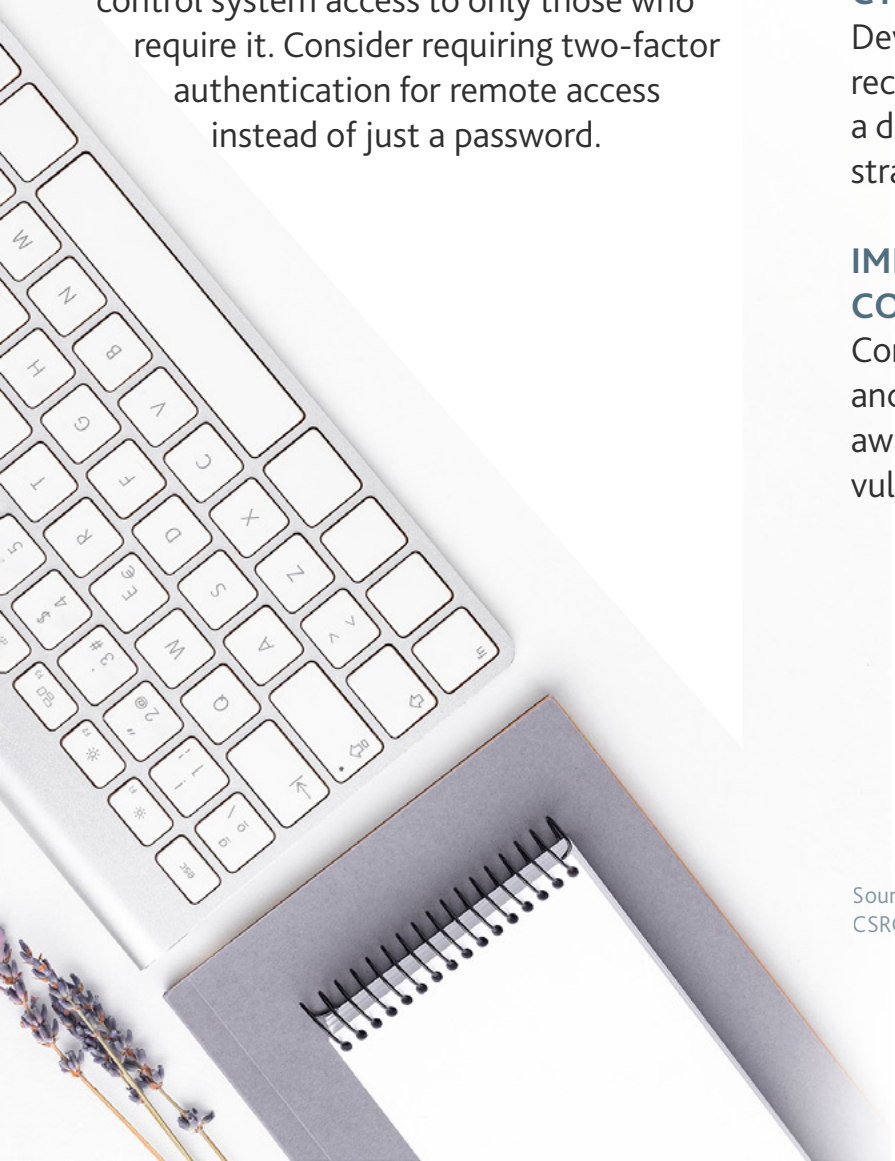
Train control system users on their cybersecurity responsibilities and look for anything unusual that may be evidence of a cybersecurity incident.

MANAGE USER ACCESS AND CREDENTIALS

Review who has on-site or remote access to your systems and revoke unnecessary access. Immediately disable accounts and revoke credentials when someone leaves the organization.

RESTRICT CONTROL SYSTEM NETWORK ACCESS AND NETWORK ACTIVITY

Implement a layered network topology with a demilitarized zone (DMZ) to restrict access to control system networks. Limit control system access to only those who require it. Consider requiring two-factor authentication for remote access instead of just a password.



MANAGE CYBERSECURITY VULNERABILITIES

Keep your assets up to date and fully patched. Prioritize patching on "PC" machines used in human-machine interfaces (HMIs), database servers, and engineering workstations. Disable unused ports and services. Implement antivirus/antimalware/antiphishing technologies whenever possible to prevent, detect, and mitigate malware, including ransomware.

IMPLEMENT APPLICATION CONTROL

The static nature of some control system assets, such as database servers, HMIs, and engineering workstations, makes them ideal candidates for running application control solutions.

PREPARE TO RECOVER FROM A CYBERSECURITY INCIDENT

Develop and implement an incident recovery plan. Plan, implement, and test a data backup and restoration system and strategy.

IMPLEMENT AND PERFORM CONTINUOUS MONITORING

Continuously monitor system boundaries and inbound and outbound traffic. Stay aware of relevant cybersecurity threats and vulnerabilities.

Source:
CSRC.NIST.GOV

COMPANY RECOMMENDATIONS

Information security is built every day with small measures applied by everyone.

ROLE MANAGEMENT
Maintain and control that information is only accessible to user profiles that genuinely need to view and modify it. For the rest, it should be restricted.

DEVICE CONTROL
Considering the wide variety of devices on the market, restrict access only to those with appropriate security tools in place.

PROTECTION AGAINST MALICIOUS CODE
To ensure that data is not affected by malicious code, all devices should have security solutions that proactively detect this type of threat.

NETWORK TRAFFIC MONITORING
Since there are devices entering the network from outside the physical office perimeter, it is necessary to monitor the type of traffic they generate.

SECURE CONNECTIONS
For remote work, implementing client-based VPN connections is most convenient, where the user runs the application, authenticating with a username and password, and even adding a second factor of authentication, creating an encrypted channel between the device and the remote network for secure data exchange.

WRITING A SECURITY POLICY
Determine the obligations and responsibilities of users regarding the use of the technologies at their disposal. Define the type of actions that can be taken and who is authorized to execute them.

EMPLOYEE AWARENESS
Education should be an important pillar so that all users are aware of the risks they may be exposed to and what precautions they should take when introducing external devices to the company.

SECURE PASSWORDS

Attackers use a variety of techniques to discover passwords, including the use of powerful tools available for free on the internet. The following advice enhances password security for your users, improving the security of your system as a result (Source: National Cyber Security Center).

HOW PASSWORDS ARE DECRYPTED...

Interception: Passwords can be intercepted as they are transmitted over a network.

Brute Force: Automated guessing of billions of passwords until the correct one is found.

Lookup: Digital cloud resources can be searched for information that can help discover your password.

Password Theft: Insecurely stored passwords can be stolen, including handwritten passwords hidden near a device.

Manual Guessing: Personal information, such as name and birthdate, can be used to guess common passwords.

Shoulder Surfing: Observing someone typing their password.

Social Engineering: Attackers use social engineering techniques to deceive people into revealing passwords.

Keylogging: An installed keylogger intercepts passwords as they are typed.

...AND HOW TO IMPROVE THEIR SECURITY!

Help users deal with "password overload"

- Use passwords only when they are genuinely necessary.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Ask users to change their passwords only if there are suspicions of compromise.
- Enable users to reset passwords easily, quickly, and cost-effectively.

Help users generate appropriate passwords.

- Put technical defenses in place to allow for simpler passwords.
- Steer users away from predictable passwords and prohibit common ones.
- Encourage users never to reuse passwords between work and home.
- Train staff to help them avoid creating easily guessable passwords.
- Consider the limitations of password strength meters. Blacklist the most common password choices.

Monitor failed login attempts, train users to report suspicious activities.
Do not store passwords in plain text format.

THE FIRST LINE OF DEFENSE: PASSWORDS

If we have a safe in our house, it's because we have important information to protect inside it. We would never think of sticking a piece of paper on the door with the correct combination to open it.

Sticking a sticky note on our computer monitor with the access password allows anyone to access, manipulate, and even steal private and confidential personal and organizational information.

If we have a safe in our house, it's because we have important information to protect inside it. We would never think of sticking a piece of paper on the door with the correct combination to open it.

Sticking a sticky note on our computer monitor with the access password allows anyone to access, manipulate, and even steal private and confidential personal and organizational information.

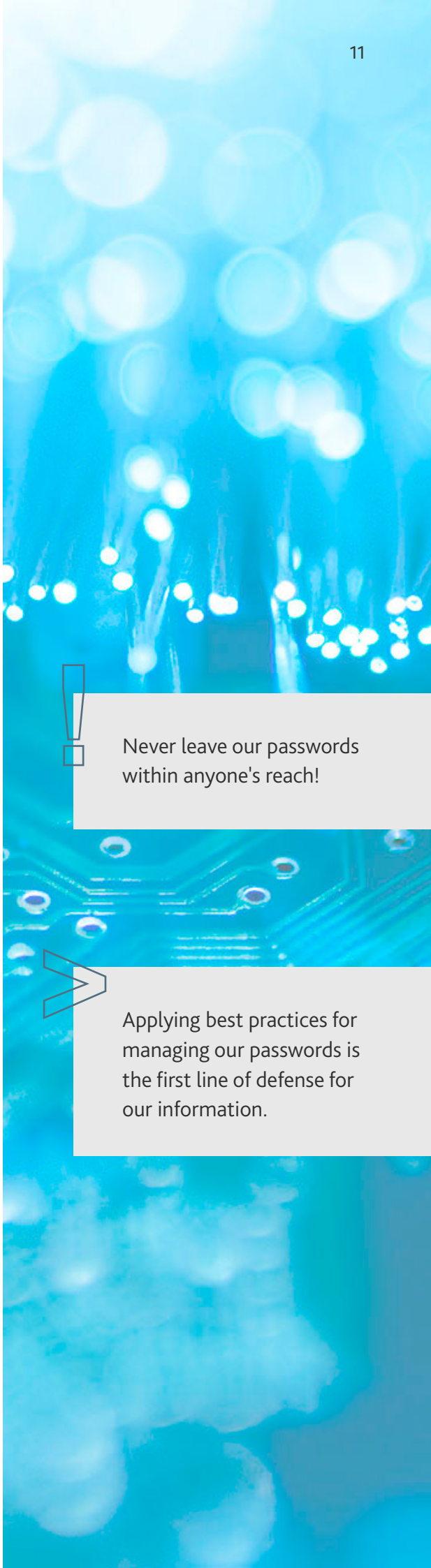
Today, almost all of us use a username and password to access websites, services, devices, or equipment. The password acts as a digital key that allows us to access all our information.

Using a secure password helps us keep our information safe and avoid falling victim to cybercrime.

Let's use different passwords for different accounts. If we always choose the same one, and someone gets hold of it, they will have access to all our accounts.

Let's use strong locks by creating passwords that are at least 10 characters long and contain lowercase letters, uppercase letters, numbers, and special symbols.

Do not publish, share, or write down our passwords in places where they can be seen by others.



Never leave our passwords within anyone's reach!

Applying best practices for managing our passwords is the first line of defense for our information.

PHISHING

Phishing is a technique used by criminals to steal our confidential information, such as usernames, passwords, credit card data, and more. Criminals attempt to deceive us by impersonating another person or organization, usually through an email.

Their messages often have an urgent tone so that the recipient doesn't think too much or analyze the situation and does what the criminal wants: open an attachment, click on a link, or reply to the message.

Criminals seek to obtain the usernames and passwords of the services we use and our personal and financial information.

With this information, they can make purchases on our behalf, transfer our money to their accounts, and impersonate us to commit crimes, among other things.

HOW CAN WE DETECT PHISHING EMAILS?

- The sender's name and email address are unknown or try to mimic a known one, for example, "Fecebook" instead of "Facebook."
- The sender is known but sends an email at an unusual time or sends something we haven't requested.
- The sender tries to make us do something urgently or within a time limit so that we don't think too much.
- The sender asks us to click on a link to get something of interest or to avoid a penalty or unpleasant situation.
- The message contains unexpected attachments, such as an invoice in our name.
- The sender requests a response containing confidential data, such as a password or credit card number.

Eventually, we will receive some phishing emails in our inbox. That's why we should be vigilant and think twice before:

- Clicking on unsolicited links.
- Downloading unexpected attachments.
- Responding to an email with our confidential information.

EMAIL

When we use our email, we expose ourselves to a variety of threats, such as SPAM and phishing, among others.

Unsolicited emails sent to a large number of recipients for advertising or commercial purposes are called SPAM. Not only can they be annoying, but they also pose a danger.

Cybercriminals can impersonate known individuals or organizations and deceive us to steal money and private information.

Emails in which they attempt to deceive us into revealing our private information are called phishing, and they are a very common threat these days.
An email from a cybercriminal can look identical to a legitimate one and can also lead us to sites identical to legitimate ones through links. To prevent falling victim to phishing, simply never provide our private information via email or through any website we reach by clicking on a link.

To protect a corporate email, it's important to avoid publishing company-associated email addresses on any website without first verifying the reputation and credibility of that website.

Some consequences of falling victim to phishing:
- Making purchases on our behalf.
- Using our identity for illegal activities.
- Receiving more phishing emails in our inbox.

When facing a SPAM or phishing email:
- Do not respond or forward the email.
- Avoid clicking on links and downloading attachments.
- Mark the email as SPAM or phishing.
- Delete the email.

It is important that we stay vigilant, exercise caution, and continually educate ourselves to prevent all the threats we face when using our email.

SAFE BROWSING

Currently, we spend a significant part of our day connected to the Internet, but we don't always act with security in mind.

We use social networks, check our email, conduct banking transactions, shop, and much more, **but it can also become a trap.**

Unfortunately, there are cybercriminals who use the Internet to commit crimes.

WHAT CAN A CYBERCRIMINAL DO IF WE FALL INTO THEIR TRAP?

- Steal information from our device, such as login credentials, banking data, or private material, among others.
- Make purchases on our behalf or transfer our money.
- Hijack our information and then demand a ransom for it.
- Commit crimes in our name, such as distributing child pornography.

FOLLOWING A FEW RECOMMENDATIONS CAN HELP US SAFELY NAVIGATE THE INTERNET:

- Keep our browser, operating system, and antivirus up to date.
- Browse trustworthy sites with a good reputation and widespread recommendations.
- Pay attention to the padlock icon next to the web address on secure sites. If it is not present, do not enter usernames or passwords.
- Avoid using public Internet connections when entering confidential information such as credit card data or home banking login details.
- Avoid clicking on ads or pop-ups. Use an ad blocker to prevent them from appearing.
- Avoid installing unknown browser add-ons.
- Avoid downloading programs, movies, or music from unofficial sites.

THE IMPORTANCE OF INFORMATION SECURITY

Information is the asset that allows us to make decisions both personally and professionally, which is why we must protect it.

Information is an essential and vital resource for our organization.

- The data we generate and/or use in our daily work.
- The systems we operate on.
- The reports we read.
- The knowledge we possess about the company.
- All of this is part of the organization's INFORMATION and must be protected.

WHAT INFORMATION SHOULD BE CONSIDERED CONFIDENTIAL?

- Personal data of clients and collaborators in general.
- Financial information.
- Product or service development projects.
- Information committed to maintaining confidentiality with a third party. Clients, partners, suppliers, etc.

Every day, we handle all kinds of information in our work and personal lives.

If we look closely, we can see that it is very valuable. Not only for us but also for malicious individuals who commit cybercrimes through the use of technology and the Internet.

To keep our private data safe from these increasingly common threats, the field of Information Security teaches us good habits to consider in our personal, family, and professional lives. Without secure behavior, cybercriminals will take advantage of us, and in addition to financial losses, we will expose the image of our organization and its clients.

WHAT CAN CYBERCRIMINALS USE THIS TYPE OF INFORMATION FOR?

- Obtain large sums of money by selling it on the black market.
- Impersonate an executive.
- Damage the image or credibility of our organization.
- Extort members of our organization.

We don't need to be security experts, but we do need to be aware of the threats we are exposed to and avoid falling for cybercriminal tricks by learning a few safe habits.

RANSOMWARE TIPS

Quick steps you can take now to **protect yourself** from the ransomware threat:

- **USE ANTIVIRUS SOFTWARE ALL THE TIME:** Configure your computer to automatically scan your emails and external storage devices.
- **KEEP YOUR COMPUTER UPDATED:** Run periodic checks to keep your computer up to date and patched.
- **BLOCK ACCESS TO RANSOMWARE SITES:** Use security products or services that block access to known ransomware sites.
- **ALLOW AUTHORIZED APPLICATIONS ONLY:** Configure the operating system or third-party software to allow only authorized applications on your computer.
- **RESTRICT PERSONAL DEVICE ACCESS:** Organizations should restrict or prohibit personal device access to official networks.
- **USE STANDARD USER ACCOUNTS:** Use standard user accounts instead of privileged administrative accounts whenever possible.
- **DISABLE PERSONAL APPLICATION USAGE:** Disable the use of personal applications and websites, such as email, chat, and social networks, from company terminals.
- **BE CAUTIOUS WITH UNKNOWN SOURCES:** Do not open files or click on links from unknown sources unless you have first run an antivirus scan or examined the links carefully.

Steps you can take now to help **recover** from a future ransomware attack:

- **BACKUP & RESTORE:** Carefully plan, implement, and test a data backup and restoration strategy, and protect and isolate backups of important data.
- **KEEP YOUR CONTACTS UPDATED:** Maintain an up-to-date list of internal and external contacts for ransomware attack scenarios, including law enforcement.
- **PREPARE AN INCIDENT RECOVERY PLAN:** Develop and implement an incident recovery plan with defined roles and decision-making strategies. External storage devices.

Source
CSRC.NIST.GOV

At **BDO**, we do what we do exceptionally well and lead wherever we are present: we have been the fastest-growing global organization in our industry for the last 10 years, serving over **775,000 clients** globally.

TALKS TO END USERS

Continuously raise awareness, educate, and train the entire organizational population.

- **PREVENTION**
  Accounts and passwords, viruses, worms, bots and botnets, trojans, backdoors, keyloggers, spyware, and phishing, among many others.

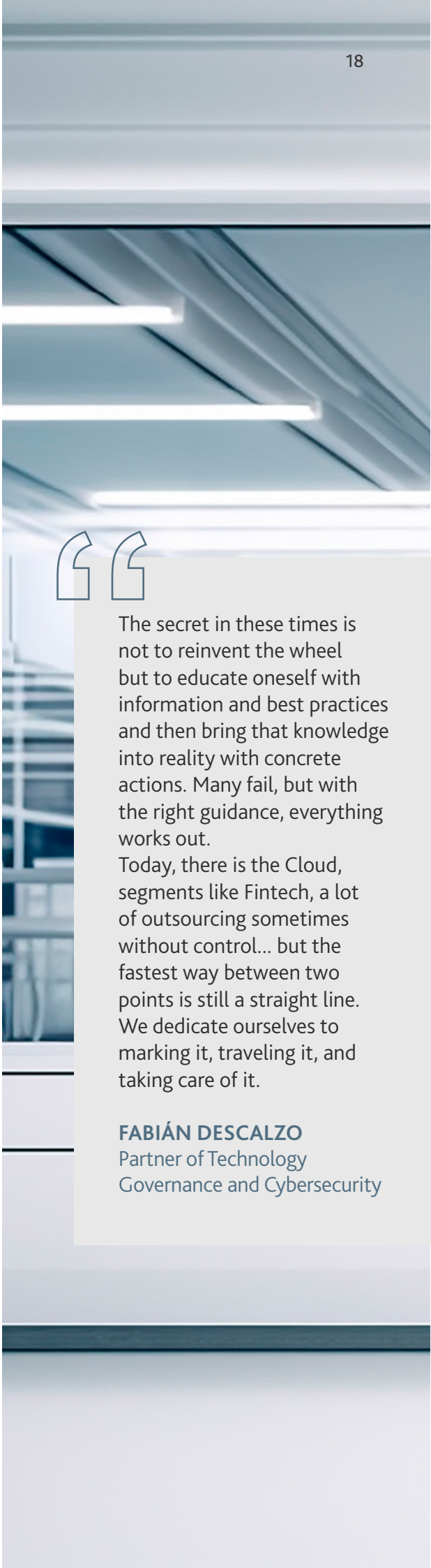
- **SAFE INTERNET USE**
  Email programs, web browsers, instant messaging, spam, file-sharing programs, resource sharing, backups. Introduction to privacy and data protection. Web privacy and security. Identity theft and incident response.

- **FRAUD**
  Social engineering, precautions when conducting banking or business transactions, chain letters.

- **INFORMATION PROTECTION**
  Back up all sensitive information stored only on personal devices.

- **PRIVACY**
  Emails, cookies, precautions with personal data on web pages, blogs and social networking sites, precautions with data stored on the hard drive, precautions with smartphones and IoT / IoP.

- **BROADBAND AND WIRELESS NETWORKS**
  Protecting a computer using broadband, protecting a network using broadband, precautions for a wireless network client.



> The secret in these times is not to reinvent the wheel but to educate oneself with information and best practices and then bring that knowledge into reality with concrete actions. Many fail, but with the right guidance, everything works out.
> Today, there is the Cloud, segments like Fintech, a lot of outsourcing sometimes without control... but the fastest way between two points is still a straight line. We dedicate ourselves to marking it, traveling it, and taking care of it.

FABIÁN DESCALZO
Partner of Technology Governance and Cybersecurity

LIMITATIONS OF AI

Explore the limitations of AI, from biases and lack of transparency to its key challenges.

1. **Bias:** AI algorithms can reflect biases due to incomplete or biased training data, resulting in unfair or discriminatory outcomes when making decisions.

2. **Lack of Transparency:** The opaque decision-making by AI algorithms makes it difficult to identify errors and biases in the results, generating uncertainty in their operation.

3. **Lack of Flexibility:** AI's limited adaptation to new or unexpected contexts is due to its dependence on training data, limiting its applicability in changing situations.

4. **Privacy and Security:** The use of sensitive data in AI raises concerns about privacy and security, increasing the risk of manipulation and sabotage of vulnerable systems.

5. **Costs and Accessibility:** The high expenses associated with the development and implementation of AI can restrict its adoption to organizations with substantial financial resources.

6. **Responsibility and Ethics:** AI's ability to make crucial decisions involves ethical dilemmas and challenges in determining responsibility in case of adverse outcomes.

7. **Interpretability of Results:** The complexity of AI algorithms can make it difficult to understand how certain results are reached, posing challenges in explaining and communicating the decisions made by the system.

WHAT IS CHATGPT?

The Powerful Artificial Intelligence Dialogue Generation Tool.

ChatGPT has been meticulously designed to excel in generating text-based dialogues, enabling it to respond and generate conversational interactions effectively. This OpenAI tool can engage in interactive conversations with users and provide relevant and coherent responses, contextualized within the flow of the conversation.

Built on the GPT (Generative Pre-trained Transformer) architecture, ChatGPT is based on the GPT-3.5 version, one of the most advanced iterations of the model. Through extensive training on web text data, the model has been educated to predict word and phrase sequences in text, giving it an understanding of human language.
Its responses are presented coherently and contextually, emulating human communication.

This conversational engine is used in various applications in the field of artificial intelligence, including virtual assistants, customer support, interactive tutorials, and content generation, among others. ChatGPT exemplifies how current technology can simulate human interactions, enhancing a variety of platforms and services with natural and accurate communication.

ETHICS IN THE USE OF CHATGPT

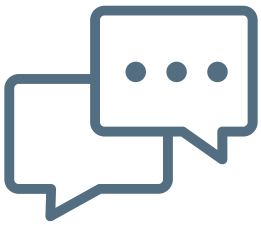
Guidelines for Responsible Interaction.

We acknowledge that this tool is invaluable for increasing efficiency in content creation, reducing time and costs. However, we should not use it without considering the potential consequences or deceptively. For ethical and proper use of ChatGPT, it is imperative to adhere to the following guidelines:

It is crucial to clarify that you are interacting with an artificial intelligence at the beginning of the conversation. This transparency is essential to set proper expectations and prevent misunderstandings.
Blindly trusting the model should be avoided. Users should understand that responses may not always be accurate or up-to-date. It is recommended to verify the information provided from additional reliable sources before accepting it as valid. If incorrect or biased information is identified in the responses, it is essential to correct it and provide accurate information. This practice is crucial to prevent the spread of misinformation online.

User responsibility extends to avoiding requesting or generating inappropriate, discriminatory, illegal, or harmful content. Using the model ethically and respectfully is essential to maintain integrity and ethics in the generated communication.

If you come across a problematic, biased, or inappropriate response, it is advised to provide feedback to the model's developers, such as OpenAI. This process contributes to continuous improvement and refinement of language models in future iterations.



SECURITY CHALLENGES IN THE USE OF CHATGPT

Exploring the Risks Posed by ChatGPT Regarding Data Security and How to Protect Yourself.

It's essential for businesses to take measures to mitigate these risks and protect themselves against potential threats.

1. **Data Security Risk:** ChatGPT's ability to collect and store extensive volumes of data increases the likelihood of security vulnerabilities, with the consequent threat of leaks and the loss of confidential information.

2. **Malware Risk:** Cybercriminals can exploit ChatGPT as a vehicle to distribute malware and other malicious programs, jeopardizing the integrity of networks and corporate systems.

3. **Privacy Risk:** The collection of personal data by ChatGPT raises concerns about privacy, potentially infringing on the confidentiality rights of the company's customers and employees.

4. **Social Engineering Risk:** ChatGPT can be exploited by cybercriminals to manipulate users and obtain sensitive information, exposing the company to significant security risks.

5. **Reputation Risk:** In the event that ChatGPT is responsible for a data breach or the loss of confidential information, the company's reputation faces a severe threat, with possible economic and legal repercussions.

10 COMMANDMENTS FOR GOVERNING CYBERSECURITY IN THE ERA OF CHATGPT

The 10 guiding governance commandments for business leaders, preventing risks, and safeguarding assets in the ChatGPT era.

1 **Risk Awareness:**
It is crucial for business leaders to have a deep understanding of the inherent risks of using ChatGPT and artificial intelligence systems. This informed awareness enables making strategic decisions that protect the organization's assets and integrity in the current digital environment.

2 **Risk Awareness:**
It is crucial for business leaders to have a deep understanding of the inherent risks of using ChatGPT and artificial intelligence systems. This informed awareness enables making strategic decisions that protect the organization's assets and integrity in the current digital environment.

3 **Ongoing Comprehensive Training:**
Empowering employees with comprehensive awareness and training programs is a fundamental pillar in the risk prevention strategy. Providing knowledge about the safe use of ChatGPT and AI encourages the ability to detect potential threats, ensuring that every team member is an active advocate for cybersecurity.

4 **Data Protection:**
Implementing robust security measures to protect the data collected in and around the ChatGPT and AI ecosystem is an unbreakable commandment. Through advanced encryption and restricted access control, a defensive barrier is created that safeguards confidential information from potential vulnerabilities and attacks.

5 **Continuous Monitoring:**
Maintaining constant supervision over the use of ChatGPT and AI serves as an active safeguard against latent threats. Real-time monitoring allows for early detection of anomalous behaviors, facilitating a swift response to any security breach attempts.

6 **Platform Updates:**
Regular and strategic updating of ChatGPT and AI software is a crucial mandate in the fight against vulnerabilities. Staying up-to-date with the latest versions and security patches reduces exposure to potential exploits and ensures a more resilient environment.

7 **Incident Preparedness:**
A solid incident response plan is essential to mitigate the effects of a potential security breach. Having clear and structured protocols for managing incidents ensures a quick and effective response, minimizing the impact in case of a breach.

8 **Rigorous Audits:**
Regular security audits allow for a comprehensive assessment of the effectiveness of implemented security measures. These periodic evaluations identify potential gaps and improvement opportunities, allowing the cybersecurity strategy to evolve with changing cybersecurity threats.

9 **Penetration Testing:**
Conducting regular penetration tests is a proactive guideline to identify and address potential weaknesses in the system. These comprehensive assessments, not only of the service itself but of all layers from end to end in the use of AI, allow for a thorough review of the infrastructure and the early detection of gaps before they can be exploited by external threats.

10 **Collaboration with Experts:**
Collaborating with cybersecurity experts provides an external and invaluable perspective to strengthen defense. The expertise of these professionals enables the early identification of emerging threats and the formulation of adaptive and effective prevention strategies. Together, they can guide the organization toward a safer and more resilient future in the digital world.

7 FUNDAMENTAL PRINCIPLES OF PRIVACY AND SECURITY

Employees can internalize the importance of cybersecurity and privacy in the digital environment, contributing to a safer and more resilient online ecosystem.

1. Digital Vigilance

Avoid Complacency: Excessive confidence in security can lead to unrecognized vulnerabilities. Maintain digital humility; assume that any system can be vulnerable, enhance control, and monitoring.

2. Data Ethics

Responsible Collection: Excessive data collection without justification can compromise users' privacy. Collect only necessary data; respect users' privacy and gather only what the business needs.

3. Emotional Control Online

React Thoughtfully: Impulsive online reactions can expose sensitive information or phishing attacks. Avoid impulsive online reactions; be wary of unsolicited links and emails. Let anxiety not govern your decisions; it's better to be slow and secure in such cases.

4. Creative Protection

Go Beyond Repetition: Imitating passwords or security practices can lead to vulnerabilities and unauthorized access. Do not imitate security practices; create unique passwords and use two-factor authentication. Two is always better than one.

5. Continuous Updates

Stay Current: Ignoring security updates can leave systems exposed to known exploits. Update regularly; security patches counter vulnerabilities. Discipline, processes, and control should be part of your daily agenda.

6. Balanced Data Management

Less Is More: Accumulating unnecessary information increases the risks of data loss and theft. Limit data accumulation; keep only what is necessary and apply security measures. A good diet ensures agility and privacy.

7. Safe Online Exploration

Browse Cautiously: Clicking on unknown links can lead to malicious websites and malware. Click with caution; verify authenticity before clicking on links.

Don't let your guard down; lack of awareness in cybersecurity is an advantage for cybercriminals.

Contacts:

FABIÁN DESCALZO
Partner in Technology Governance
and Cybersecurity
fdescalzo@bdoargentina.com

LAURA DANGELO
Director of Technology Governance
and Cybersecurity
ldangelo@bdoargentina.com

www.bdoargentina.com