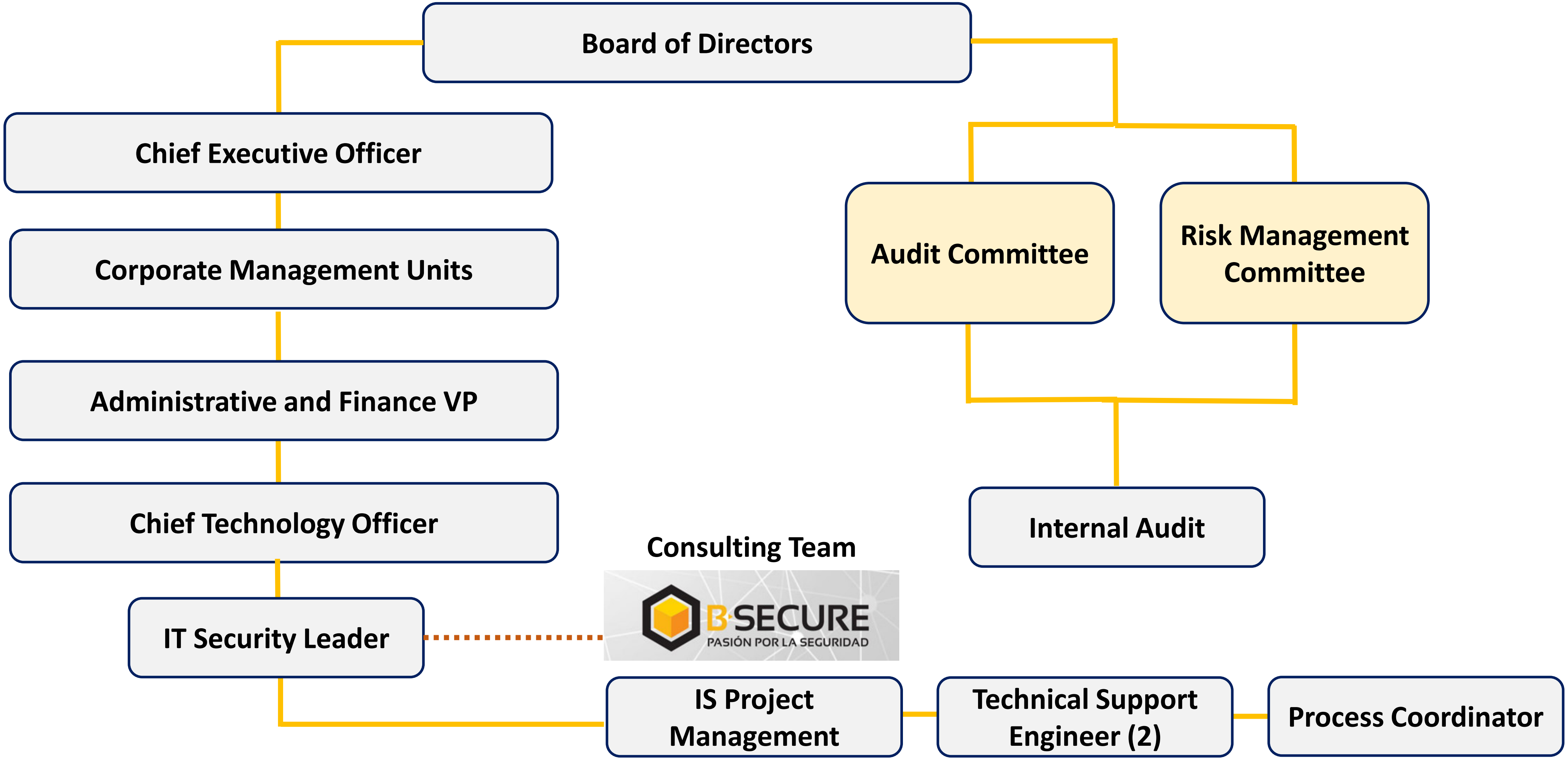
INFORMATION SECURITY MANAGEMENT SYSTEM

INFORMATION SECUTIY GOVERNANCE



Board of Directors

Chief Executive Officer

Corporate Management Units

Administrative and Finance VP

Chief Technology Officer

IT Security Leader

Audit Committee

Risk Management Committee

Internal Audit

Consulting Team

B·SECURE
PASIÓN POR LA SEGURIDAD

IS Project Management

Technical Support Engineer (2)

Process Coordinator

COMMITTEE RESPONSABILITIES

Validate, approve and authorize the implementation of actions, activities, projects and policies related to computer and information security, in terms of the characteristics of the business, the organization, its location, its assets, technology.

Validate and approve a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities to manage information security risks.

Validate and approve the management of new resources for Computer and Information Security activities or projects.

Be aware of the results of investigations into information security incidents.

Have knowledge about procedures for monitoring and reviewing IT and information security issues.

COMMITTEE RESPONSABILITIES

Validate and approve the security plans developed.

Validate and approve risk acceptance criteria and acceptable risk levels.

Ensure that internal audits are carried out at planned intervals and know the results.

Approve and review the scope, objectives and strategies of Information Security.

Approving and periodically reviewing security policies and standards.

Validate the integration of the Information Security Management System with the other systems of the organization.

ACCOMPAIMENT CONSULTING RESPONSABILITIES

Prepare the minutes of the committee meetings and verify their formalization by the members

Summon the members of the committee to the ordinary and extraordinary sessions

Timely submit the agenda of each committee

Serve as an interlocutor between third parties and the committee

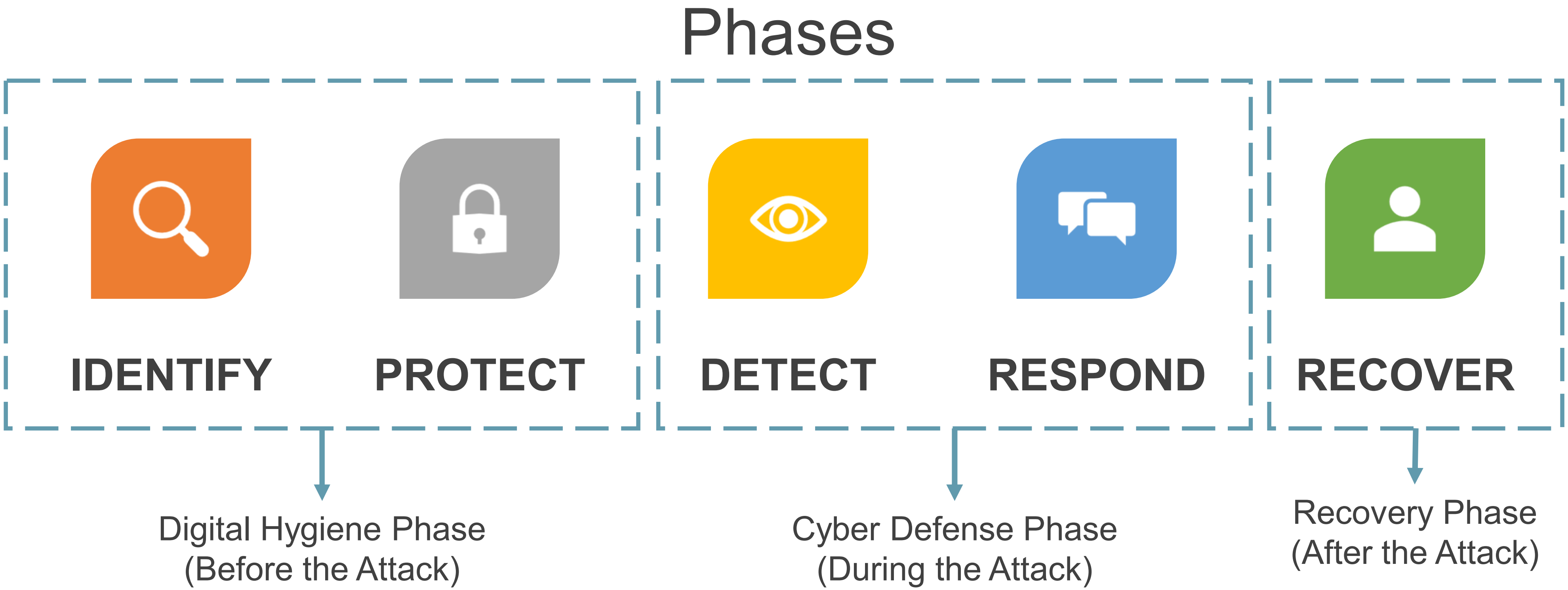
Follow up on committee commitments

Submit reports required by the committee.

PRINCIPAL ROLES AND RESPONSABILITIES

Name of the rol	Information Security Responsabilities
Top Management	This role is responsible for overseeing and ensuring information security within the organization, including reviewing and approving the corresponding policies, supporting the implementation of the Information Security Management System (ISMS), and providing the necessary resources for its compliance. Additionally, it must promote an organizational culture focused on information protection and ensure the proper dissemination of policies to all employees and stakeholders who access or handle information.
Internal Audit	Audit the Information Security Management System. · Review previous audit reports. · Ensure that security audits are conducted with the required frequency. · Submit the reports resulting from the audits to the ISMS.
IT Security Leader	Develop, promote, and maintain the information security policy. · Propose new objectives related to information security. · Develop and maintain the information security regulatory framework and ensure its compliance. · Define and propose to the Information Security and Privacy Committee the scope and boundaries of the ISMS in terms of the business characteristics, organization, location, assets, and technology.

NIST CYBERSECURITY GOVERNANCE FRAMEWORK



Source: https://www.ftc.gov/es/tips-advice/business-center/small-businesses/cybersecurity/nist-framework-es

INFORMATION SECURITY INCIDENT ESCALATION PROCESS

Step	Responsible	Key Actions	Expected Outcome
1. Notification	Employee / Contractor / Third Party	- Identify potential incident - Notify Help Desk (tool, email, Teams, phone) - Register incident with minimum details (who, when, what, where)	Incident reported and documented
2. Escalation	Help Desk	- Categorize incident (security vs. IT request) - Use knowledge base - Escalate to Information Security Leader if critical	Case assigned and escalated according to criticality
3. Analysis (Categorization and Priorization)	Information Security Leader	- Classify and prioritize incident (Annex A/B) - Identify affected assets - Notify asset owners - Escalate to IT Management if DRP required	Incident classified, prioritized, and communicated
4. Containment, Eradication & Recovery	InfoSec Leader + IT Admins	- Contain/isolate systems - Eradicate root cause - Restore systems - Seek external support if needed	Incident contained, root cause eliminated, services restored
5. Post-Incident Activities	Information Security Leader	- Document (risk, root cause, actions, evidence) - Notify Legal, Audit, HR, etc.	Lessons learned and corrective actions implemented
6. Management	Information Security Leader	- Review process annually - Monitor indicators - Generate preventive and corrective actions	Continuous improvement of incident management process

INFORMATION SECURITY BUSINESS CONTINUITY PLAN

Business Continuity and Disaster Recovery Plan

Business Continuity Plan (BCP)

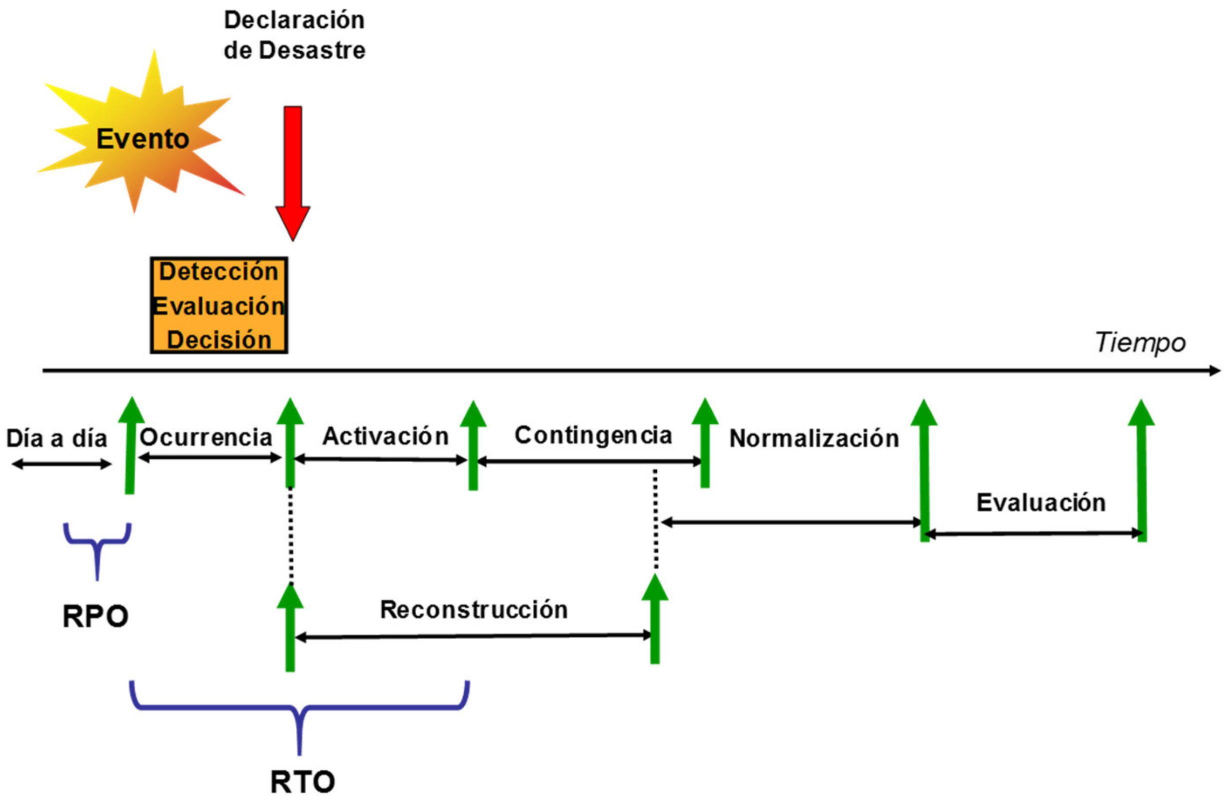
It is a set of procedures that allow the organization to preserve the operational continuity of its critical business processes in the event of a contingency situation.

Disaster Recovery Plan (DRP)

It is a set of procedures that allow the organization to preserve the continuity of the critical IT systems that support the critical business processes of the company in the event of a contingency situation.

Colombina IT Recovery Strategy

- **Recovery Parameters:**
- Recovery (RTO) = 24 hrs. (unique for all platforms)
- Maximum age of the information(RPO) = 2 hrs.



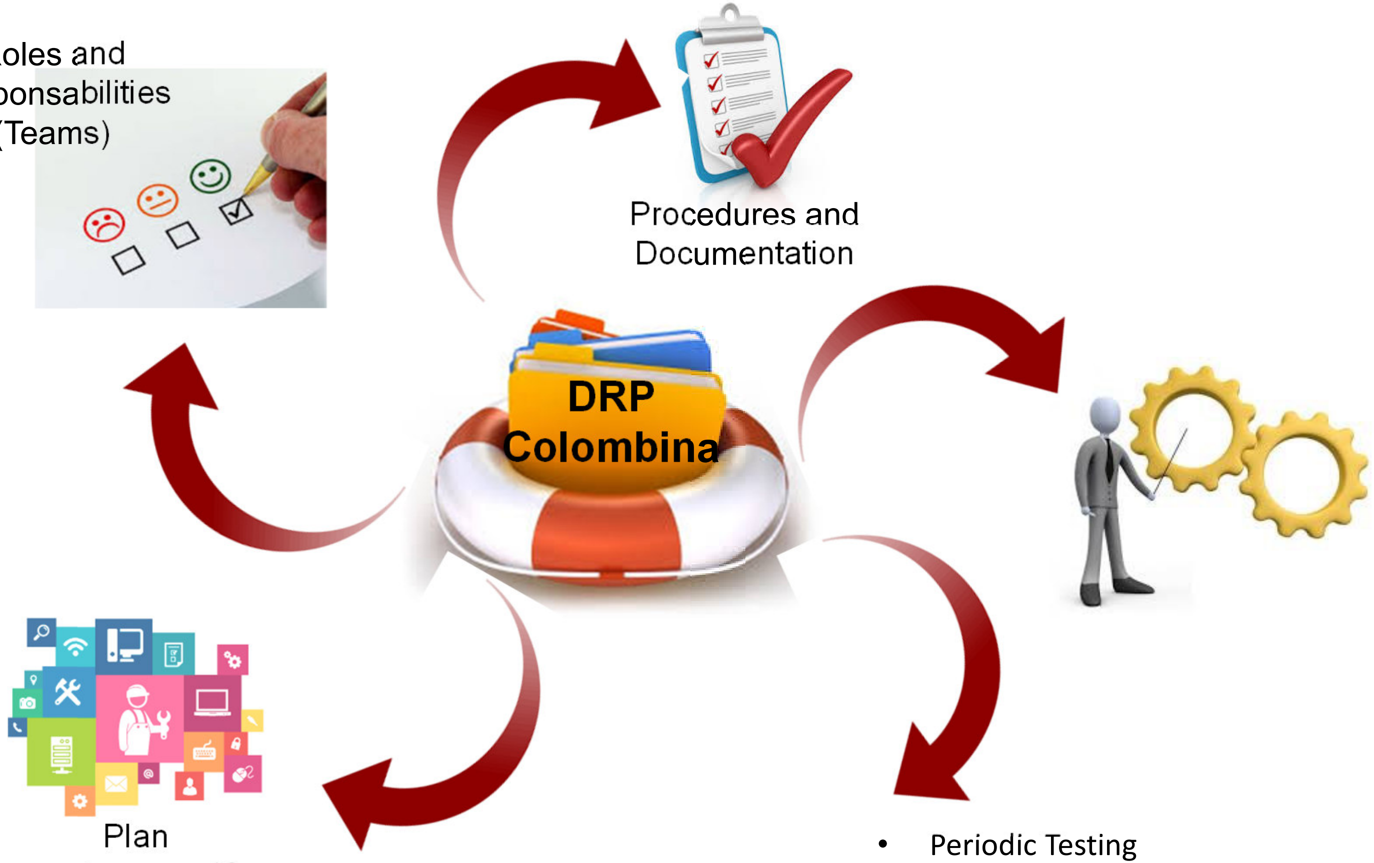
- Human Resources: The personnel required for IT recovery is organized as:
- Colombina Recovery Groups
- IBM Recovery Teams

- Technical and operational IT recovery procedures: The execution of each one of them is in charge of the respective Recovery Groups and Teams

- Other processes / procedures: The Plan has another set of documents related to management, notification, registration, etc.

- Backup processes in the CcA: The current scheme for production environments in CELTA will be maintained.

Colombina Disaster Recovery Plan (DRP)



Roles and Responsabilities (Teams)

Procedures and Documentation

Plan Maintenance (As of Jan 2016)

- Periodic Testing
- Operational (partial successful during 2015)
- Desktop (Nov 2015 successful)

General Objectives

Have an organized set of documents that contain the processes and procedures to follow and the information required so that, in a disaster situation, Colombina can:

- Maintain business continuity, through the recovery of critical business processes supported by the current IT recovery solution.

- Restore the operability of IT and telecommunications environments within predetermined recovery windows

- Minimize the number of decisions that mitigate the loss of information and money

- Plan at a high level what would be the strategies to repair, replace or enable the affected IT production environments in the shortest possible time

- Have an internal organization with the capacity, resources and procedures required to recover critical IT operations.

Plan Premises

- Colombina has defined a set of systems whose criticality imposes a comprehensive recovery solution.
- Colombina has defined her IT recovery strategy for these systems.
- The recovery solution based on said strategy will be in charge of Colombina, through the services contracted with IBM and other providers.
- It is assumed that the implemented recovery strategy will enable basic services to be enabled within the defined recovery window for critical business processes.

Plan Exclusions

- The activities for the recovery of the business areas, which are in Colombina's Business Continuity Plans (BCP), current or new to be created, and synchronized with what is established by the DRP.
- Recovery activities and procedures at other sites and other Colombina activities are outside the scope of the DRP.
- The recovery of jobs to attend to the business in alternative processing and / or attention places.

Contingency Process

IT processing under contingency:

- It starts once the Activation Stage is finished, after which the services are activated.
- Although there is no established deadline for the duration of this Stage, which will depend on the consequences of the event, the maximum estimated time is 6 weeks.

4 – Reconstruction Process:

- ➢ **IT Service Options**>> Retorn of processing to the site of origin CELTA (IBM)
- ➢ **Equipamiento de TI** (Hw & Sw & Nw) >> Original and/or equivalent equipment

5 – Normalization Process:

- ➢ **Recovery Teams** >> The same original members
- ➢ **Period of the month to normalize**>> During the second weekend of the month

Evaluation Process

- During each previous Stage, it is foreseen in the respective Action Plans that each of the Teams and Recovery Groups document, in specific formats, the most significant news and incidents that have occurred.

- In this Stage, a compilation of said information and a subsequent analysis of the entire recovery process will be developed jointly.

- The results will be included in a Final Report, which will summarize the achievements of the recovery process, together with the applicable recommendations for optimizing the IT recovery strategy and / or its DRP.

- This Final Report will be presented to the Colombina Contingency Evaluation Committee.

INFORMATION SECURITY VULNERABILITY ANALYSIS

VULNERABILITY ANALYSIS OBJECTIVES

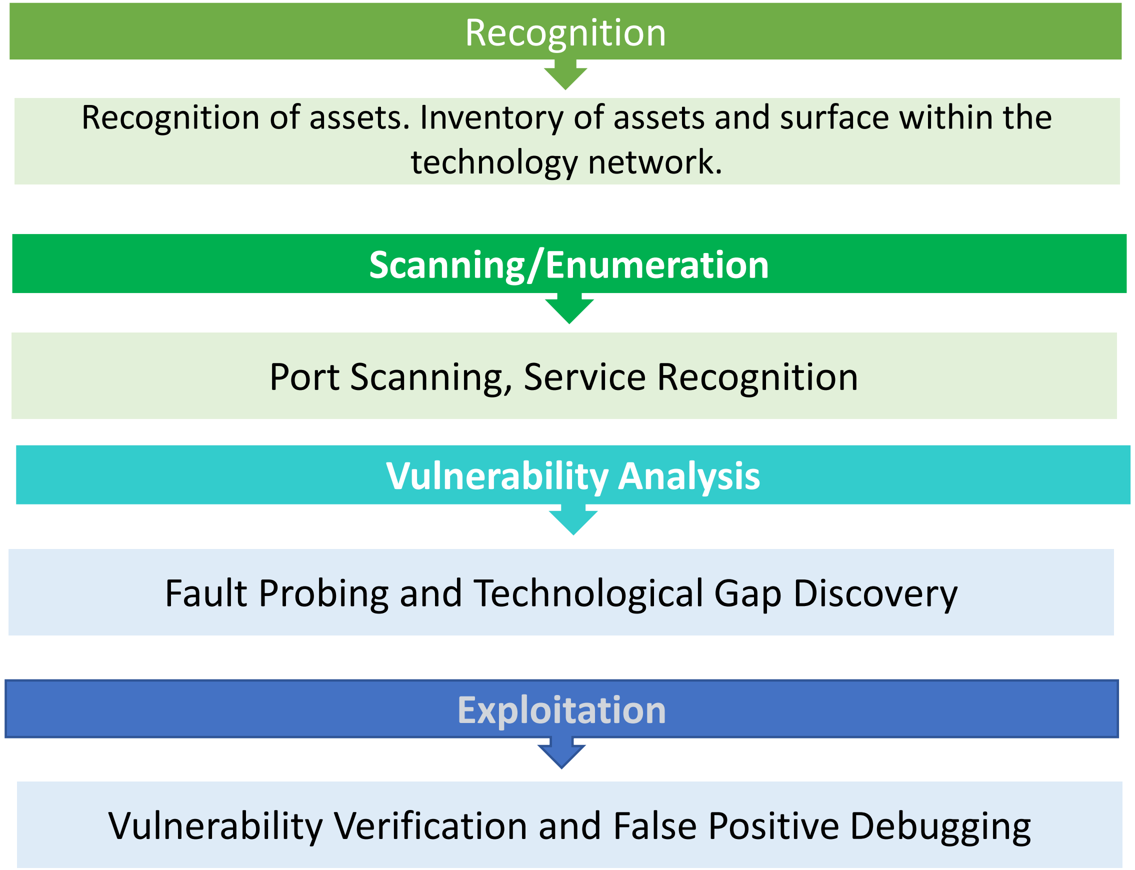
- Assess comprehensively the current state of security in the designated technological assets. Through this activity, the goal is not only to identify existing weaknesses but also to provide valuable recommendations that enable the alignment of security controls with a proactive approach.

- Evaluate the current level of information security awareness among employees, in relation to potential risks and everyday situations that could compromise the organization’s security.

- The scope of the tests includes ethical hacking (internal and external assets) and social engineering tests (phishing and vishing).

VULNERABILITY ANALYSIS METHODOLOGY

Through the annual exercise of vulnerability analysis and penetration testing, the current level of security of the company's technological infrastructure is evaluated. This activity generates recommendations that enable proactive and sustainable approaches, benefiting the processes supported by the Information Security Leader. The main objective is to identify opportunities for improvement in terms of confidentiality, integrity, and availability of information, ensuring the effective management of the Information Security Management System (ISMS).



Recognition

Recognition of assets. Inventory of assets and surface within the technology network.

Scanning/Enumeration

Port Scanning, Service Recognition

Vulnerability Analysis

Fault Probing and Technological Gap Discovery

Exploitation

Vulnerability Verification and False Positive Debugging

INFORMATION SECURITY INTERNAL AUDITS

INTERNAL AUDIT PROCESS

Review of accesses in the ERP (SAP S/4 HANA) to ensure they are authorized, aligned with job functions, and with proper segregation of duties

Verification of regulatory compliance: Personal Data Protection and software licensing.

Review of certain DRP processes.

Review of automated controls in the main business processes within the ERP.

Participation in selected IT projects to verify information integrity and new functionalities.

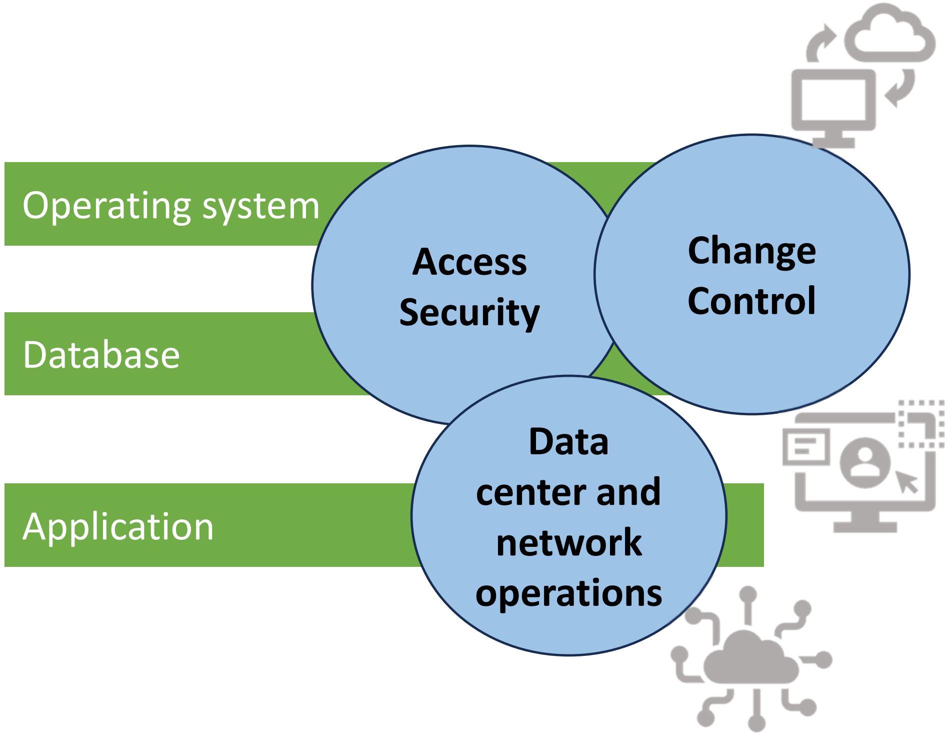
Review of cybersecurity controls

INFORMATION SECURITY EXTERNAL VERIFICATION

EXTERNAL VERIFICATION

External verification is conducted annually with the objective of assessing the effectiveness and reliability of the technological systems and practices that support business operations. Compliance and effectiveness tests are performed on the implemented controls, and potential risks that may affect business continuity are analyzed.

According to the review of general computer controls at Colombina S.A. regarding the infrastructure, significant progress has been observed in strengthening internal control. Out of thirty (30) audited controls, only four (4) presented findings, with the final results being satisfactory. This demonstrates the company's ongoing commitment, year after year, to ensuring robust controls within the IT department across different areas.



INFORMATION SECURITY AWARENESS TRAINING TO EMPLOYEES

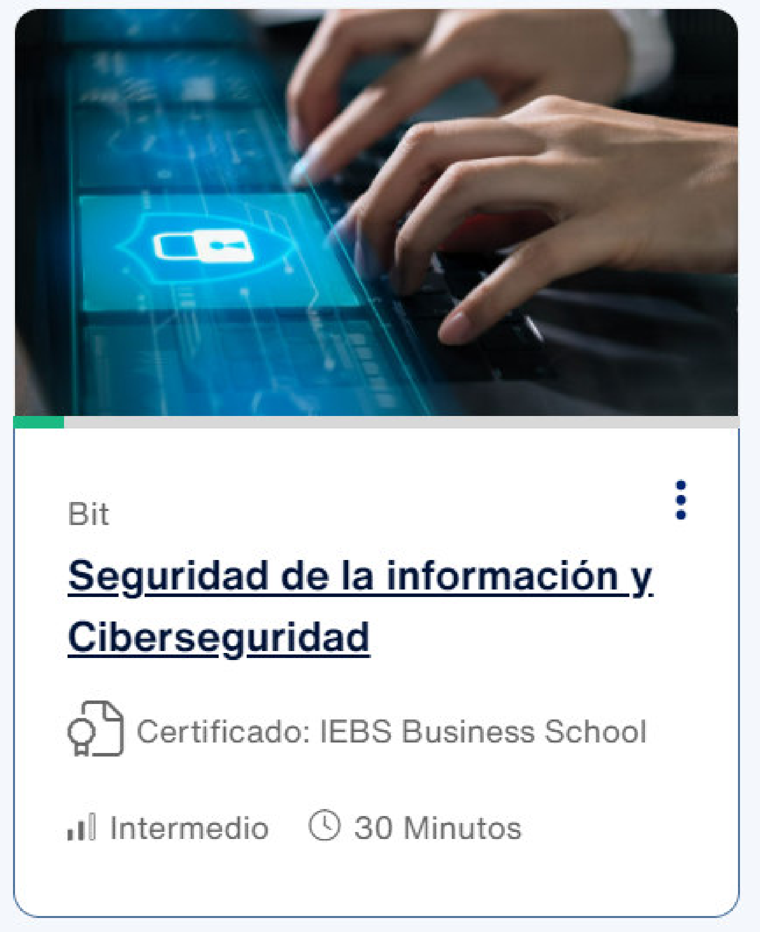
Universidad Corporativa
Colombina

Colombina Corporate University Course
Information Security and Cybersecurity

At the end of this course, employees will be able to:

- Recognize the main risks, threats, and vulnerabilities that affect information systems.
- Differentiate between the concepts of information security and cybersecurity.
- Value company information as a strategic asset.
- Explain the principles of confidentiality, integrity, and availability of information.
- Apply preventive measures at work to protect information.

More than 2,200 employees completed this virtual course.



Bit

Seguridad de la información y Ciberseguridad

Certificado: IEBS Business School

Intermedio 30 Minutos

Universidad Corporativa Colombina

Colombina Corporate University Course Personal Data Protection

At the end of this course, you will be able to:

- Explain what personal data is and how it is classified.
- Argue the value of personal data protection laws.
- Describe the principles and rights underlying personal data protection laws in Latin America.
- Justify the need for establishing data processing policies in companies.

Microbits:

Microbit 1: Habeas data: a right for all

Microbit 2: Personal data

Microbit 3: Data processing policy

Bit | ¡Completo!

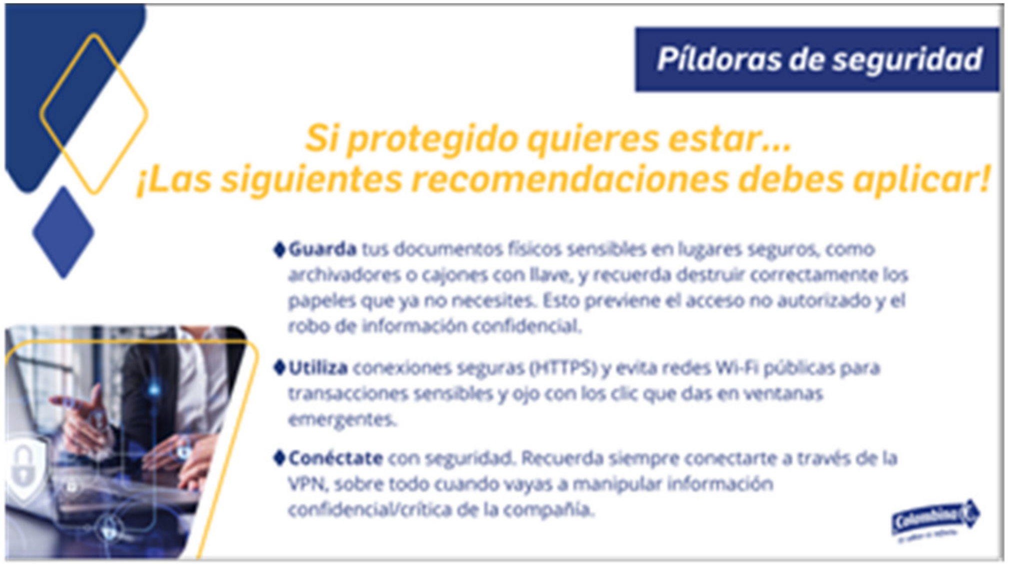
Protección de datos personales

Certificado: BSL Business School Lausanne

More than 2,470 employees completed this virtual course.

E-MAIL CAMPAINGS

Security Tips


Píldoras de seguridad

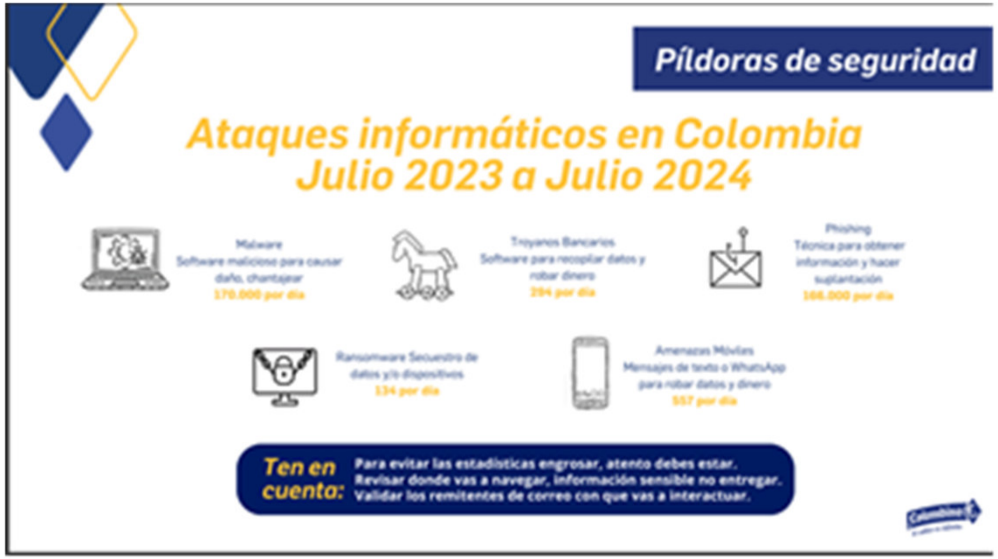
Si protegido quieres estar...
¡Las siguientes recomendaciones debes aplicar!

- **Guarda** tus documentos físicos sensibles en lugares seguros, como archivadores o cajones con llave, y recuerda destruir correctamente los papeles que ya no necesites. Esto previene el acceso no autorizado y el robo de información confidencial.
- **Utiliza** conexiones seguras (HTTPS) y evita redes Wi-Fi públicas para transacciones sensibles y ojo con los clic que das en ventanas emergentes.
- **Conéctate** con seguridad. Recuerda siempre conectarte a través de la VPN, sobre todo cuando vayas a manipular información confidencial/crítica de la compañía.

If you want to stay protected… make sure to follow these recommendations!

- Keep your sensitive physical documents in secure places, such as locked filing cabinets or drawers.
- Use secure connections (https) and avoid public Wi-Fi networks for sensitive transactions.
- Connect safely. Always remember to log in through the VPN.

Cibersecurity Tips


Píldoras de seguridad

Ataques informáticos en Colombia
Julio 2023 a Julio 2024

Malware
Software malicioso para causar daño, chantajear
170.000 por día

Troyanos Bancarios
Software para recopilar datos y robar dinero
294 por día

Phishing
Técnica para obtener información y hacer suplantación
166.000 por día

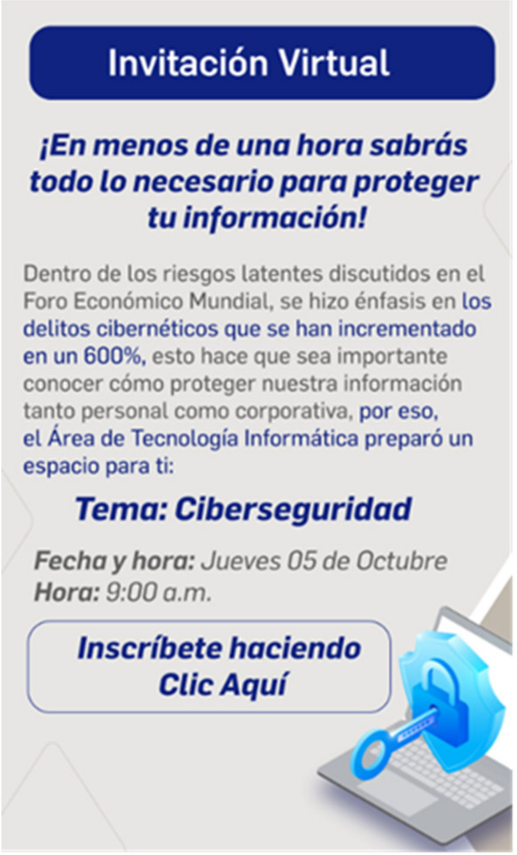
Ransomware Secuestro de datos y/o dispositivos
134 por día

Amenazas Móviles
Mensajes de texto o WhatsApp para robar datos y dinero
557 por día

Ten en cuenta: Para evitar las estadísticas engrosar, atento debes estar. Revisar donde vas a navegar, información sensible no entregar. Validar los remitentes de correo con que vas a interactuar.

Data on cyberattacks in Colombia from July 2023 to July 2024

Virtual Invitation



Invitación Virtual

¡En menos de una hora sabrás todo lo necesario para proteger tu información!

Dentro de los riesgos latentes discutidos en el Foro Económico Mundial, se hizo énfasis en los delitos cibernéticos que se han incrementado en un 600%, esto hace que sea importante conocer cómo proteger nuestra información tanto personal como corporativa, por eso, el Área de Tecnología Informática preparó un espacio para ti:

Tema: Ciberseguridad

Fecha y hora: *Jueves 05 de Octubre*
Hora: *9:00 a.m.*

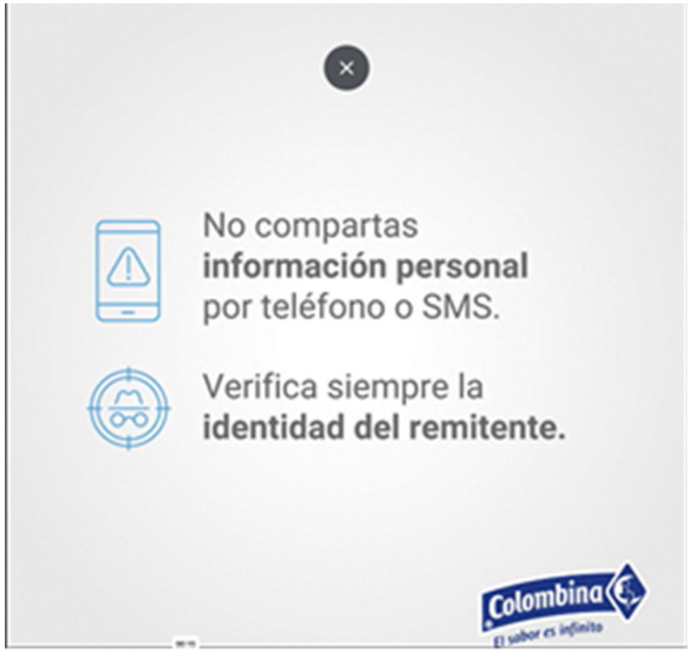
Inscríbete haciendo Clic Aquí

In less than an hour, you will learn everything you need to know to protect your information!

Among the latent risks discussed at the World Economic Forum, special emphasis was placed on cybercrime, which has increased by 60%. This makes it essential to understand how to protect both our personal and corporate information. For this reason, the IT Department has prepared a special session for you:

Topic: Cybersecurity
Date and Time:

Register by clicking here



No compartas **información personal** por teléfono o SMS.

Verifica siempre la **identidad del remitente.**

Colombina
El sabor es infinito

Do not share personal information over the phone or via text message.

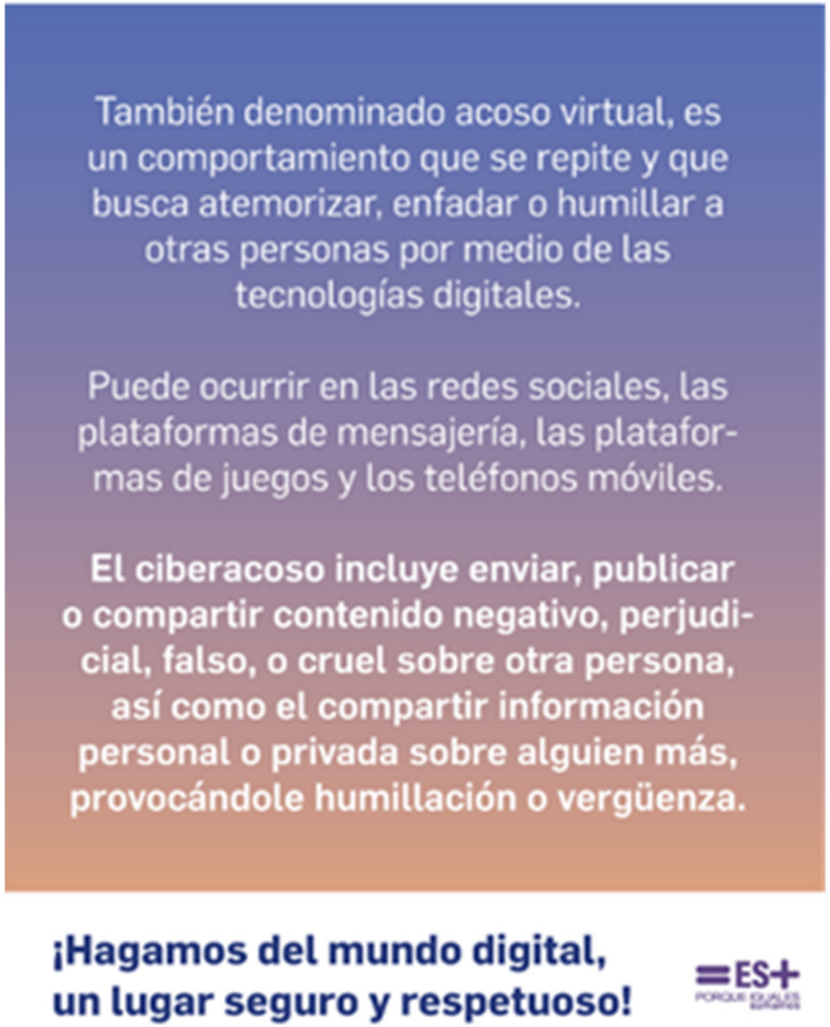
Always verify the sender’s identity.

¿Ciberbullying?

Also known as cyberbullying, it is a repeated behavior intended to intimidate, anger, or humiliate others through digital technologies.

It can occur on social networks, messaging platforms, gaming platforms, and mobile phones.

Cyberbullying includes sending, posting, or sharing negative, harmful, false, or cruel content about another person, as well as sharing someone’s personal or private information, causing them humiliation or embarrassment.



También denominado acoso virtual, es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas por medio de las tecnologías digitales.

Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles.

El ciberacoso incluye enviar, publicar o compartir contenido negativo, perjudicial, falso, o cruel sobre otra persona, así como el compartir información personal o privada sobre alguien más, provocándole humillación o vergüenza.

¡Hagamos del mundo digital, un lugar seguro y respetuoso!

=ES+