Virtual meeting on cyber security

Cyber incident response and recovery

Joshsua James González Díaz

Adviser

Operational Risks and Cybersecurity Dependency

Financial Superintendence of Colombia

Bogotá D.C., November 4th 2020

External Circular 007 of 2018

Minimum requirements for cybersecurity management

General requeriments

- ✓ Standards for managing Cybersecurity
- ✓ Implement a SOC
- ✓ Active participation of the Directors board and Senior Management.
- ✓ Secure software development
- ✓ Information Security (IS) and Cybersecurity (CS) management indicators

1. Prevention

Design and implement appropriate controls to ensure information (IS) security and cybersecurity (CS) .

- ✓ Set up a specialized SI and CS unit.
- ✓ Adjust the BCP.
- ✓ Implement a Security Information and Event Management (SIEM) .

2. Protection y detection

Design and implement activities to identify CS events.

- ✓ Procedures to identify CS incidents.
- ✓ Manage vulnerabilities.
- ✓ Monitor the technology platform to identify unusual activity.

3. Response and communication

Design and implement plans and procedures to mitigate CS incidents.

- ✓ Incident response procedures.
- ✓ Report cyber attacks to ColCERT.
- ✓ Report to financial consumer and the SFC of CS incidents.
- ✓ Mechanisms to recover information systems.

4. Recovery and learning

Update resilience plans and restore affected services.

- ✓ Review and update security systems configurations after an incident.
- ✓ Socialize and share lessons.

sfc
Superintendencia Financiera de Colombia

Assess the maturity level of digital security, establish opportunities for improvement, update plans and strategies for cybersecurity management.

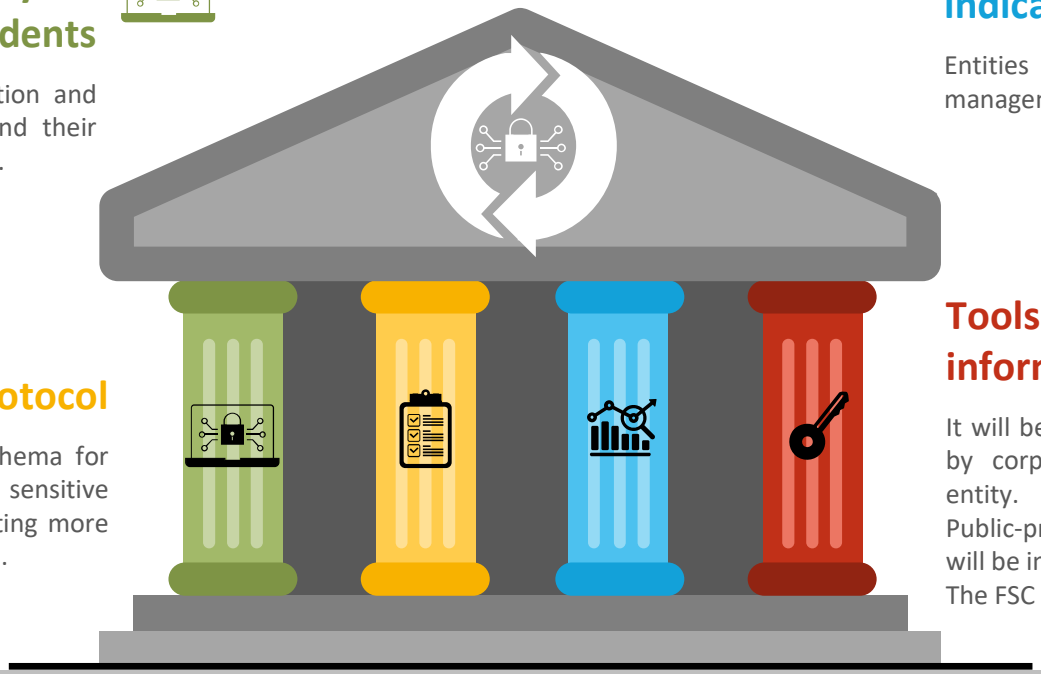
New External Circular
Sharing Information

Unique Taxonomy Cyber Incidents

Basic guidelines for the identification and classification of cyber incidents and their reporting using a common language.

Cybersecurity management indicators

Entities must report the IS and CS management indicators every 3 months.



TLP Protocol

Provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration.

Tools for share information

It will be done initially by email and through by corporate account established by the entity.
Public-private key encryption mechanisms will be implemented.
The FSC will manage the keys.

External Circular 007 of 2018
Minimum requirements for cybersecurity management

sfc
Superintendencia Financiera de Colombia

Incident Report Requirement

How entities do it

- Entities report incidents that affect the confidentiality, integrity and availability of information.
  - Phone Call Report
  - Email
  - Update reports
  - Official Report

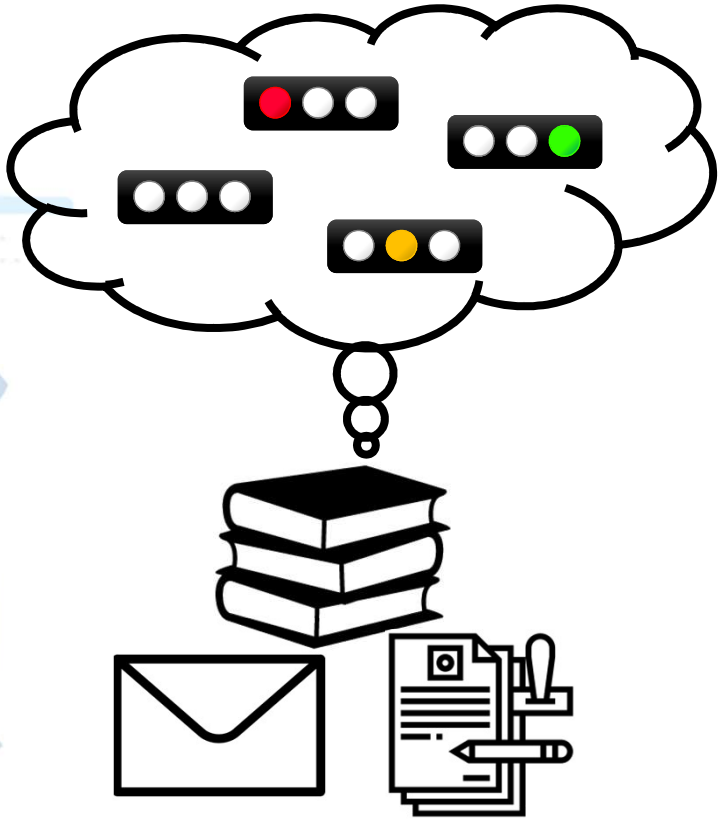
- With the new circular they will do:
  - Phone Call report
  - Encrypted email
  - Unique Format
    - TLP
    - Unique Taxonomy of Cyber Incidents (UTCI)

Traffic Light Protocol (TLP)

It was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s).

TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration. TLP is not a "control marking" or classification scheme.

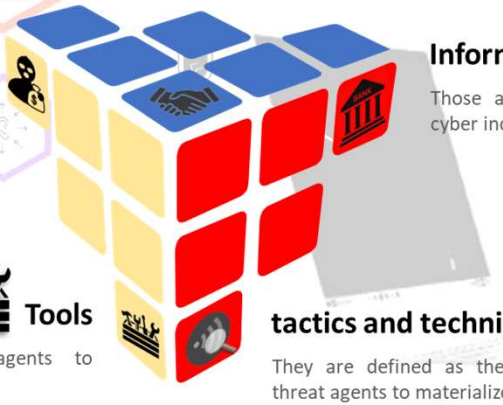
With the new external circular all entities must use this protocol to report incidents and share cybersecurity information.



sfc
Superintendencia Financiera de Colombia

Unique Taxonomy Cyber Incidents - UTCI

- Basic guidelines necessary to report cyber incidents, offering a standardization and common language in the identification process.
- Composed by nine (9) different categories and five (5) elements.



Purpose

This element may provide a clear identification of the incident.

Threat Agents

Also called as a threat actor, is any person or "thing" that acts (or has the power to act) to cause, carry, transmit, or summit actions to explode a vulnerability.

Information Assets

Those assets which are affected by the cyber incident.

Tools

Elements used by threat agents to materialize an incident.

tactics and techniques*

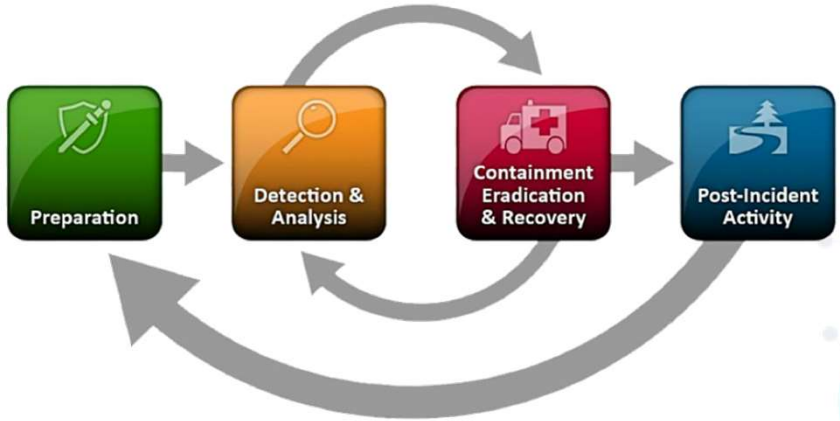
They are defined as the actions of the threat agents to materialize the incident.

- Content abuse
- Intrusions
- Information Security
- Vulnerabilities
- Fraud
- Service availability
- Information gathering
- Malicious code
- Others

sfc
Superintendencia Financiera de Colombia

Response and Follow-up Cyber Incidents

Protocol to supervise incident management

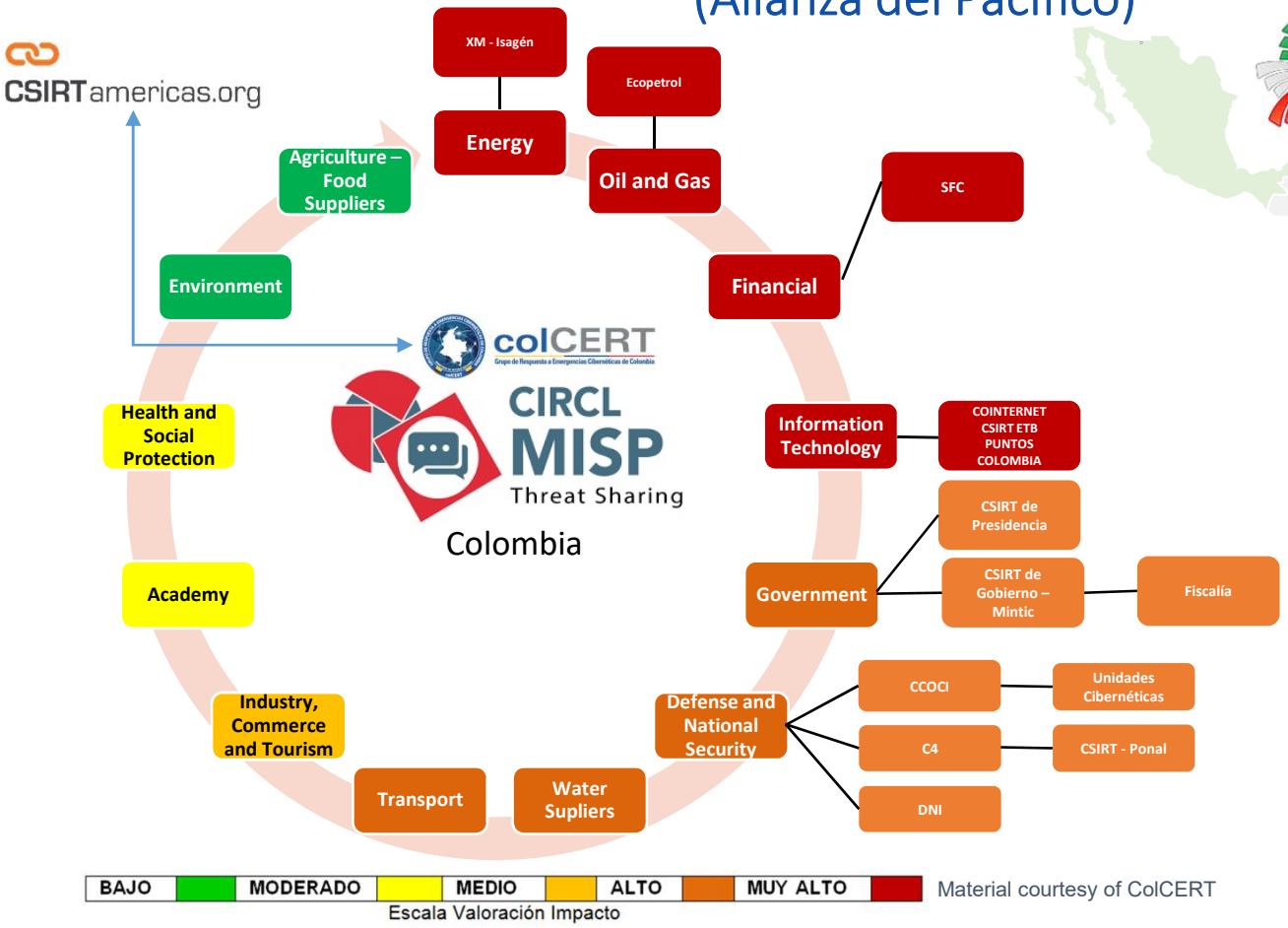


Extraído de: NIST 800-61 Computer SecurityIncident Handling Guide R2
Disponible en: https://bit.ly/2x3qmLQ

- Based on the NIST 800-61 Computer Security Incident Handling Guide standard, 5 response phases were created.
- They are aligned with the stages described in external circular 007 of 2018:
  - Response and communication
  - Recovery and learning

Project MISP Local and Internacional Connection

(Alianza del Pacifico)



Material courtesy of ColCERT

Alianza del Pacífico

OAS More rights for more people

OBJECTIVES

-Evaluate the current situation of the MISP installation
-Detect improvements in the implementation and quality of information and collaboration
-Define integration opportunities with other cybersecurity solutions

ACTIVIDADES

-Initial workshop to identify requirements of each country.
-Current configuration review
-Integration with other MISPs at the region.
-MISP security review.
-Evaluate integration with other cybersecurity solutions.

sfc Superintendencia Financiera de Colombia

Other Expectations

- Unique platform for incident reporting.
- Guide for monitoring incident management in cloud architecture.
- Consolidate the implementation of the MISP.
- Simulation of a cyber incident that affects one or more financial entities considered as Critical Infrastructure, in coordination with the other countries of the Pacific Alliance.

- Improve communication channels with supervisors from other countries on the continent to share:
  - Regulation
  - Methodologies
  - Supervision guidelines
  - Good practices
  - Tools
  - Success cases
  - Technical support
  - Training

sfc
Superintendencia Financiera de Colombia

superintendencia.financiera

@SFCsupervisor

+Superfinanciera

/superfinancieracol

Thank You

super@superfinanciera.gov.co

www.superfinanciera.gov.co