## Table of Contents

## 1. OBJECTIVE

Establish Ecopetrol S.A.'s process for the identification, analysis, prioritization and remediation of vulnerabilities in the assets and technological components that support business processes, including, but not limited to: firewalls, routers, switches, servers and orchestration platforms such as Kubernetes.

This procedure aims to reduce the risks associated with cybersecurity, such as unauthorized access to systems, database exfiltration, theft of credentials, and exposure of personal or financial information, through the implementation of technical and operational controls that guarantee the protection of the organization's technological infrastructure.

## 2. GENERAL CONDITIONS

### 2.1 SCOPE

The scope of this document applies to all components of technological infrastructure (IT), software and telecommunications equipment, as well as prioritized applications and covers all vulnerabilities following a prioritization order and action plans stipulated in this document.

### 2.2 TERMS AND DEFINITIONS:

- Countervailing Controls: Controls applied indirectly on the vulnerable system
- Remediation: The act of correcting a vulnerability or eliminating a threat.
- Prioritized Applications: VTI Risks and Controls - Prioritized Applications - All Items (mcas.ms)
- IT: Information Technology
- Vulnerability: It is a weakness or failure in an information system.
- Emerging vulnerability: A newly discovered weakness or flaw in a system, software, hardware, device, or protocol

## 3. DEVELOPMENT

**BACKGROUND**

Vulnerability management supports risk detection activities. However, it must be borne in mind that it is necessary to establish a solid base with people and processes, as well as the interdisciplinary interaction of work teams that guarantee the success of the activities.

6 steps are defined to perform and execute vulnerability management. These steps are described below:

1. Planning: Planning the vulnerability management process.
2. Discovery: Detection of vulnerabilities in systems and processes within the scope of this procedure.
3. Analysis, vulnerability assessment and reporting of results: Assessment of gaps and recommendations for risk remediation.
4. Definition of remediation plans: Generate an action plan that indicates when and in what way remediation actions should be applied.

5. Remediation: These actions must be executed in the established times to reduce exposure times and reduce the risks of non-compliance.
6. Verification of effectiveness: It is verified that the actions of the remediation plans have been implemented correctly and that the gaps have been closed.

## 3.1 Vulnerability Management

### 3.1.a Planning

In the case of productive platforms, the vulnerability analysis must be carried out, at least, on the prioritized applications. Exceptions to this obligation are those applications that operate under PaaS, SaaS or IaaS models, which are not under the responsibility and management model of the Head of Platforms and Connectivity, which must have the respective SOC2 report as evidence of compliance, provided by the service/POD leaders to the Cybersecurity and Cyber Defense Management (**GCY**)). The inventory of the prioritized applications must be provided by the Corporate Compliance Directorate (**RCU).**

The tools used in vulnerability analysis must have specific purpose hardware and be approved to the CVE (Common Vulnerabilities and Exposures), or any other information resource established at the regulatory level, and updated to the date of their use.

The Head of Platforms and Connectivity (**JPL**), the Digital Solutions Management (**GSD**) or the area that is responsible for the administration of the IT infrastructure and applications, must guarantee the provision of the necessary access that allows the effective execution of the vulnerability analysis process. Such access must be sufficient to ensure complete visibility of all services, components and resources associated with the application or infrastructure under analysis, in order to identify possible security weaknesses in a timely manner.

The frequency of vulnerability scans is listed below:

| Scan Type | Description | Frecuencia |
|---|---|---|
| Scans of Prioritized infrastructure | IT and telecommunications infrastructure | Every other day |
| Prioritized application scans | In pre-productive environments | Before entering production (CTI-G-028 Guide for the management of cybersecurity in projects and initiatives) |
| Prioritized application scans | In productive environments | Quarterly or on-demand |
| Scans of Infrastructure No prioritized | In pre-productive and productive environments | Quarterly or on-demand |
| Domain Scanning External | ASM (Attack surface management) | Monthly |

**Table 1 - Frequency of scans**

3.1.b Discovery

The transition team must ensure that any new project or project that requires an update complies with the vulnerability management process.

It is necessary that all process of registrations to services (new network segments, new architectures, among others), go through the transition process so that the Cybersecurity and Cyber Defense Management (**GCY)** has knowledge to be able to carry out the corresponding vulnerability management.

The Head of Platforms and Connectivity (**JPL**), as well as the headquarters attached to the Digital Solutions Management (**GSD**), must provide the Cybersecurity and Cyber Defense Management (**GCY),** at least once a month, with an updated inventory of the assets to be analyzed, along with the information of the person in charge assigned to each one. This measure aims to ensure comprehensive visibility of the vulnerabilities associated with the organization's assets.

Taking into account the inventory of network segments, the Cybersecurity and Cyber Defense Management (**GCY)** may randomly execute network scans at its own discretion to identify assets that are not part of the official inventory and, if necessary, scale with JPL and Ecopetrol's SOC.

Service/POD leaders will need to ensure that all prioritized infrastructure and applications comply with this procedure, regardless of their operating environment. This includes both cloud environments under service models such as SaaS, IaaS, PaaS and Infrastructure as Code (IaC), in accordance with the cloud service provider's shared responsibility model as On-Premise environments. Compliance with this process is mandatory to ensure the timely identification and mitigation of security risks in business-critical technology assets.

SaaS and PaaS applications prioritized as SOX applications must have the SOC2 report (Certification Report of Cloud Providers, evaluated by an external entity that guarantees the application of controls that guarantee cybersecurity, availability, privacy, integrity of processing, and confidentiality of their services).

Service/POD leaders will be responsible for managing and safeguarding such report, and shall make it available to the vulnerability management process when required as part of the inputs required for the assessment of technological risks.

3.1.c Analysis, vulnerability assessment and reporting of results

Vulnerability management is a process that has different types of analyses that allow us to know the vulnerabilities of applications or infrastructure and its criticality. The different types of analyses available for execution are listed below.

| Type of analysis | Description |
|---|---|
| External infrastructure analysis | Analysis of the perimeter, networks or hosted or externally available infrastructure, associated with the prioritized applications, with the aim of identifying possible vulnerabilities accessible from the Internet. |
| Internal Infrastructure Analysis | Analysis of the prioritized internal technological and physical infrastructure within the organization. The vulnerability management tool agent must be installed on each asset or, failing that, the credentials for authentication will be provided. |
| In-depth application analysis | Deep authenticated scans to identify security vulnerabilities, including integration developments such as APIs and others that may be susceptible to security breaches. |
| Application Source Code Analysis (Document GUIDE FOR MANAGING BACKLOG AND BOARDS IN AZURE DEVOPS) | Analysis of the application's source code is run during application development to identify problems in the code that could cause potential vulnerabilities. |

**Table 2 - Types of vulnerability analysis**

All systems shall be subjected, where technically feasible or required, to an authenticated analysis of internal infrastructure prior to their implementation in the production environment. This analysis aims to identify and mitigate vulnerabilities before the system is put into operation.

Once the systems are deployed in the production environment, they must be maintained under a continuous analysis scheme, as part of the permanent vulnerability management process, in order to guarantee the security and resilience of the technological infrastructure.

When the available source code has modifications, during the transition phase the vulnerabilities of the entire code must be evaluated again, in order to mitigate new exposures before being transferred to production environments. When source code is available, applications must undergo source code analysis before the updated code is moved to production if there has been a change to the application code. (Document GUIDE FOR MANAGING BACKLOG AND BOARDS IN AZURE DEVOPS)

3.1.d Definition of remediation plans

The order of attention and remediation of vulnerabilities prioritizes the level of severity of the vulnerability and the criticality of the asset that presents the vulnerability.

I. The partner in charge of the asset analyzes whether it is possible to perform remediation through tests in laboratory environments or validations with manufacturers.

II. The partner must make the formal request for the standard change for vulnerability remediation implementation, as established by the CTI-G-12 TRANSITION AND CHANGE PRACTICE GUIDE. This change must have a schedule for the monthly implementation of vulnerability remediation (includes cybersecurity patches) this schedule must be at least one year.

III. The ally in charge of the asset, before the authorized change window, must generate the backup of the asset or component to be remediated, in order to secure the information in case there are inconveniences at the time of carrying out the activity and the roll back process must be executed.

IV. During the authorized change window, the ally in charge of the asset must generate a trust restart prior to remediation, as long as the installation of patches or updates requires a restart, in order to ensure that the environment does not have inconveniences associated with the changes made by the closure of the vulnerabilities. In case of having a technical or business justification for not doing it, this must be documented in the change, in case the implementation of the remediation of the vulnerability fails.

V. In the event that it is not possible to comply with the remediation within 30 days of the last update, the service/POD leader must formally submit a technical justification to the Cybersecurity and Cyber Defense Management, indicating an estimated upcoming datefor its execution.

VI. The ally assigned to each asset must apply the implementation of vulnerability remediation according to the vulnerability prioritization process, in accordance with the activities indicated in the previous points.

VII. Functional and service/POD leaders must maintain continuous monitoring of applications to ensure that there are no negative events related to the remediation of vulnerabilities.

VIII. The Head of Platforms and Connectivity will be in charge of monitoring the cloud providers that are responsible for managing the vulnerabilities that arise in the layers that correspond to them according to the contracted cloud model, whether it is IaaS, PaaS and according to their baseline.

**Remediation times:** The vulnerabilities detected must have a remediation plan and its implementation will be carried out by the partners responsible for the assets, the prioritization of the activities will be given according to the severity identified for each vulnerability and the remediation times are contemplated in the following table:

| Severity of vulnerability | Remediation Time |
|---|---|
| Critical Vulnerabilities | Action plan in 1 week, maximum remediation in 1 month. |

| | |
|---|---|
| High Vulnerabilities | Action plan in 1 week, maximum remediation in 1 month. |
| Medium Vulnerabilities | Action plan in 2 weeks, maximum remediation in 3 months |
| Action plan in 2 weeks, maximum remediation in 3 months | Action plan in 2 weeks, maximum remediation in 3 months. |

**Table 3 - Remediation times**

En caso de requerir una mayor segregación de priorización por el alto volumen de vulnerabilidades a remediar, se recomienda tener en cuenta las siguientes preguntas, las cuales, en caso afirmativo They will assign greater prioritization:

1. Does the asset correspond to infrastructure that supports a prioritized application?
2. Does the prioritized application meet all 3 prioritization characteristics at the same time? That is, it is: SOX, BCP and DPS .
3. Is the asset exposed to the internet?
4. Does the vulnerability have a public exploit?
5. Can the vulnerability be exploited without an authentication process?
6. Is the vulnerability being actively exploited by cybercriminal groups?
7. If the vulnerability is exploited, is it possible to execute code remotely (RCE)?
8. If the vulnerability is exploited, is it possible to cause a denial of service (DoS)?
9. Does vulnerability remediation not require asset reboot?

If the asset does not have specific compensatory controls (e.g., protected by WAF or IPS) that help prevent exploitation of the vulnerability, it should be assigned higher prioritization.

3.1.e Verification of effectiveness

It is important during the vulnerability management process to verify the effectiveness of the compensatory controls implemented or the validation of remediations, therefore, it is required:

That the service/POD leader or the project leader or the asset owner requests the execution of the vulnerability re-test of the infrastructure or application to ensure that the vulnerabilities have been successfully mitigated.

## 3.2 Exception handling

Exception handling applies only when:

- A manufacturer has not remediated or patched a particular vulnerability and is under investigation.
- When the cost of closing the vulnerability exceeds the project budget. This must be formally justified by the service/POD leader or functional leader or the project leader.
- When the implementation of vulnerability remediation affects the business process.
- Due to technological obsolescence.

In this case, the ally in charge of the asset must justify the cause, and make a record where it is evidenced:

- Result of the risk analysis that implies the non-remediation of the vulnerability.
- Identification of use cases that allow us to know what could happen if the vulnerability is compromised.
- Compensatory controls or actions taken to mitigate the impact that the compromise of vulnerability could have.
- Work plan for the implementation of compensatory controls, this must contain at least the activities to be executed, those responsible for the execution and the closing dates for the activities.
- The minutes must be signed as follows to:

| **Vulnerability Classification** | **First passed** | **Second approver** | **Third Approver** | **Aware** |
|---|---|---|---|---|
| Review | Servant Leader (POD) and Functional Leader | Head of Digital Solutions and Head of Functional Leader Department | Manager of the areas involved | Cybersecurity and Cyber Defense Manager<br><br>Vulnerability Management Process Leader |
| High | Servant Leader (POD) and Functional Leader | Head of Digital Solutions and Head of Functional Leader Department | | Cybersecurity and Cyber Defense Manager<br><br>Vulnerability Management Process Leader |
| Media | Servant Leader (POD) and Functional Leader | | | Vulnerability Management Process Leader |
| Low | Servant Leader (POD) and Functional Leader | | | Vulnerability Management Process Leader |

- Una entregada de manera formal el acta firmada a la Gerencia de Ciberseguridad y Ciberdefensa, la cual será responsable de la aprobación de la justificación técnica de la no posible mitigación de la vulnerabilidad, custodia del documento y del ajuste correspondiente en la herramienta de gestión de vulnerabilidades, con el fin de que dicha justificación sea categorizada como una excepción temporal.

- Exceptions recorded in the vulnerability management tool shall be monitored on a quarterly basis, in order to assess their validity and determine the continuity or revocation of their status as an exception.

Additionally, it must be guaranteed through Ethical Hacking tests that the compensatory controls implemented reduce the risk of this vulnerability being exploited.

3.2.a Project vulnerability management

In the production environment, which encompasses infrastructure, applications, and domains (URLs), if vulnerabilities are identified that are not related to the scope of the project, the project will be allowed to be deployed to production once the critical, high, and medium vulnerabilities within its scope have been fixed. However, this authorization will be conditional on the existing vulnerabilities in production having a remediation plan. In situations where there is no defined plan, the service/POD leader should be asked to define one, especially for critical and high vulnerabilities. The monitoring of the plan will be carried out through the working groups managed by the Cybersecurity and Cyber Defense Management in the company of the application leader, the service leader and the ally.

### 3.3 Roles and responsibilities

Vulnerability scans can only be carried out by the Cybersecurity and Cyber Defense Management. For cases where such tests are considered invasive, they must be previously agreed with the Digital Infrastructure Management in order to prevent impacts on the operation.

Emerging or newly discovered vulnerabilities (zero day) must be communicated by email immediately to service leaders for their respective remediation process, which will proceed to an emergency change, as established by the CTI-G-12 TRANSITION AND CHANGE PRACTICE GUIDE.

In the case of code analysis of programming languages not supported by the tools defined by Ecopetrol, the relevance of contracting the tests with a third party must be evaluated.

| | Activity | Digital Infrastructure Management | Cybersecurity and Cyber Defense Management | Project Leader | Digital Solutions Management |
|---|---|---|---|---|---|
| General | Running vulnerability scans | I | R, A | I | |
| | Communication of emerging vulnerabilities to service leaders for management. | I | R, A | I | I |
| | Evaluate the relevance of contracting the tests with a third party, in the case of code analysis of programming languages not supported by the tools defined by Ecopetrol | C | I, C | R | C |
| Planning | Network and system administrators must provide sufficient access to allow the vulnerability scanning engine to scan all services provided by the system. | R, A | I | C | |
| Discovery | Ensure that any new project or one that requires an update complies with the vulnerability management process. | | C | R, A | |

| | Activity | Digital Infrastructure Management | Cybersecurity and Cyber Defense Management | Project Leader | Digital Solutions Management |
|---|---|---|---|---|---|
| | Notify all process of registrations to services (new network segments, new architectures, among others) to the cybersecurity and cyberdefense management in order to be able to carry out the corresponding vulnerability management. | R, A | C | I | R, A |
| | Have an inventory of the assets to be analyzed and the person responsible for the remediation management of the findings for each of them in order to have complete visibility of the vulnerabilities of the organization's assets. | R, A | I | | I |
| | Ensure the prioritized infrastructure and applications must provide the vulnerability management process either in the cloud (for SaaS, IaaS, PaaS and IaC services according to the cloud service provider's shared responsibility model) or on-premise. | R, A | C | | R, A |
| | Ensure that SaaS and PaaS applications prioritized as SOX applications have the SOC2 report (Cloud Provider Certification Report, evaluated by an external entity that guarantees the application of controls that guarantee cybersecurity, availability, privacy, integrity of processing, and confidentiality of their services) | | I | R, A | |
| Definición de planes de remediación | Ensure that cloud service providers manage vulnerabilities that arise at the appropriate layers in accordance with the contracted cloud model, whether IaaS, PaaS, or SaaS and in accordance with their baseline. | R, A | I | I | |
| Remediación | Ensure that critical, high, and medium criticality vulnerabilities are remediated | R, A | I | I | R |
| Verificación de la efectividad | Request the execution of the vulnerability retest of the infrastructure or application to ensure that the vulnerabilities have been closed. | I | C, I | R, A | I |
| Manejo de excepciones | Ensure that the compensatory controls implemented prevent the vulnerability from being exploited. | R | C, I | R, A | R |

**Table 4 - RACI Matrix**

**R: Responsible**
**A: Executor of the activity**
**C: ConsultedI: Informed**

### 3.4 Information processing

In accordance with Ecopetrol's information classification provisions, vulnerability reports correspond to **Classified** information, for this reason the labels and controls provided in the CTI-M-005 Information Security Manual must be used.

### 3.5 APPLICABLE REGULATIONS

- https://cve.mitre.org/cve/ - Programa de identificación de CVE®
- https://www.sans.org/reading-room/whitepapers/threats/paper/34180 - Implementación de un proceso de vulnerabilidades
- SecurityFocus BugTraq en http://www.securityfocus.com - Priorización de vulnerabilidades según su CVE
- Open Source Vulnerability Database en http://www.osvdb.org/ - Base de datos de vulnerabilidades
- https://nvd.nist.gov/ - Base de datos de vulnerabilidades
- ISO 27001 - A.12.6 - Manejo de vulnerabilidades
- DevOps - Backlog (mcas.ms)

## 4. CONTINGENCIES

**N/A**

## 5. ANNEXES

### VERSION LIST

| Previous Document | | | |
|---|---|---|---|
| **Version** | **Fecha dd/mm/aaaa** | **Document Code and Title** | **Changes** |
| 1 | 03/08/2021 | SGY-G-009 Guide for Technical Vulnerability Management | Emisión del documento |
| 1 | 24/06/2024 | CTI-G-043 Guide for Technical Vulnerability Management | Coding and management system changes |
| **New Document** | | | |
| **Version** | **Date dd/mm/aaaa** | **Cambios** | |
| 1 | 24/07/2025 | The type of document is modified, from guide to Procedure for the Management of Technical Vulnerabilities | |

**Elaborated:**

**Practice Leader:**
Juan Felipe López juanfe.lopez@ecopetrol.com.co

**Dependency:**
Corporate Vice Presidency of Science, Technology and Innovation
Cybersecurity and Cyber Defense Management


| Electronically reviewed by: | Electronically approved by: |
|---|---|
| **Erica Alexandra Reina Ceballos**<br>Cybersecurity Professional<br>Registro: E0287174<br>**Cybersecurity and Cyber Defense Management** | **Elkin Ferney Quintero Gómez**<br>Cybersecurity and Cyber Defense Manager<br>Registro E0307304<br>**Cybersecurity and Cyber Defense Management** |

*Documento firmado electrónicamente, de acuerdo con lo establecido en el Decreto 2364 de 2012, por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.*
*Para verificar el cumplimiento de este mecanismo, el sistema genera un reporte electrónico que evidencia la trazabilidad de las acciones de revisión y aprobación por los responsables. Si requiere verificar esta información, solicite dicho reporte a Service Desk.*