



System and Organization Control 3 (SOC 3) Report

Report of the Cirion Technologies Housing/Colocation, Hosting and DEC 3 Services System Relevant to Security and Availability

For the Period November 1, 2022 through October 31, 2023



Contents

Section I - Report of Independent Accountants	2
Section II - Management's Report of its Assertions on the Effectiveness of Its Controls Over the Cirion Technologies Hosting, Housing and DEC3 Services system Based on the Trust Services Criteria for Security and Availability.....	4
Attachment A – Description of Cirion Technologies Housing, Hosting and DEC3 Services System.....	5
Attachment B – Principal Service Commitments and System Requirements.....	13



Pistrelli, Henry Martin y Asociados S.R.L.
25 de mayo 487 - C1002ABI
Buenos Aires, Argentina

Tel: (54-11) 4318-1600/4311-6644
Fax: (54-11) 4510-2220
ey.com

Section I - Report of Independent Accountants

To: Cirion Technologies Data Center, Cloud & Security Services Vice Presidency

Scope:

We have examined management's assertion, contained within the accompanying Management's Report of its Assertions on the Effectiveness of Its Controls Over the Cirion Technologies Hosting, Housing and DEC 3 Services system Based on the Trust Services Criteria for Security and Availability (Assertion), that Cirion Technologies' controls over the Cirion Technologies Hosting, Housing/Colocation and DEC 3 Services System (System) were effective throughout the period 1 November 2022 to 31 October 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security and availability (applicable trust services criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Management's Responsibilities

Cirion Technologies' management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Cirion Technologies Housing/Colocation, Hosting and DEC 3 Services System (System) and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Cirion Technologies' relevant security and availability policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Cirion Technologies' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.



Inherent limitations:

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Cirion Technologies' principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.


Opinion:

In our opinion, Cirion Technologies' controls over the system were effective throughout the period 1 November 2022 to 31 October 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

December 19th, 2023

C.A.B.A, Buenos Aires

PISTRELLI, HENRY MARTIN ASESORES
S.R.L.
C.P.C.E.C.A.B.A. T° 1 F° 12


Pablo Dandois (19 de dezembro de 2023 15:13 GMT-3)

Pablo A. Dandois
Socio
Contador Público Nacional (U.B.A.)
C.P.C.E.C.A.B.A. T° 205 - F° 152



Section II - Management's Report of its Assertions on the Effectiveness of Its Controls Over the Cirion Technologies Hosting, Housing/Colocation and DEC3 Services system Based on the Trust Services Criteria for Security and Availability

December 19th, 2023

We, as management of, Cirion Technologies are responsible for:

- Identifying the Cirion Technologies Hosting, Housing/Colocation and DEC 3 Services System (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period 1 November 2022 to 31 October 2023, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security and availability set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Very truly yours,

Gabriel del Campo
Gabriel del Campo (19 de dezembro de 2023 12:51 GMT-3)

Gabriel Del Campo
VP Data Center
Cirion Technologies

Attachment A – Description of Cirion Technologies Housing/Colocation, Hosting and DEC3 Services System

About Cirion Technologies

Cirion Technologies provides local, national and global communications services to enterprise, government and carrier customers. Cirion Technologies' comprehensive portfolio of secure, managed solutions includes fiber and infrastructure solutions; IP-based voice and data communications; wide-area Ethernet services; video and content distribution; data center and cloud-based solutions. Cirion Technologies serves customers in more than 450 markets in 45 countries over a global services platform anchored by owned fiber networks on three continents and connected by extensive undersea facilities. For more information, please visit www.ciriontechnologies.com.

The following services are offered as part of the Data Center business line: managed services, hosting, housing, office space, storage utilities, security solutions, backbone Data Center, monitoring and mail & messaging. To support its transactions in the different Latin American countries, Cirion Technologies has Data Center facilities at the following locations:

ARGENTINA

Buenos Aires (BUE1)
Mendoza (MEN1)
Córdoba (COR1)
Rosario (ROS1)

ECUADOR

Guayaquil (GUA1)
Quito (QUI1)
Quito (QUI2)

BRAZIL

São Paulo (SAO1) (*)
Curitiba (CUR1)
Rio de Janeiro (RIO1)

PERU

Lima (LIM1) (*)

CHILE

Santiago (SAN1) (*)

VENEZUELA

Caracas (CAR1)

COLOMBIA

Bogotá (BOG2) (*)
Bogotá (BOG1)
Cali (CAL1) (*)

MEXICO

Ciudad de México (MEX1)

PANAMÁ

Ciudad de Panamá (PAN1)

(*) Data Centers covered by this report.

Components of the System:

The following Cirion Technologies services are covered in this report:

- Housing/Colocation

The Housing/Colocation services enable a company to place its mission critical equipment in a high-availability computing center with distinctive infrastructure characteristics, featuring a private area for the development of its business, with reliable high-performance connectivity to the inter-carrier networks and the Internet. Environmental conditions are ensured by applying controls, and which are monitored to provide a suitable environment.

- Hosting

The main objective of the Cirion Technologies Hosting services is to offer customers dedicated hardware and a secure environment for the installation of their applications, avoiding the need for these customers to perform maintenance and operating tasks. Environmental conditions are ensured by applying controls, and which are monitored to provide a suitable environment.

The current Hosting service is based on leading-edge servers, fully installed with base software, and configured in the most flexible way to cater to the needs of customers.

Cirion Technologies also has an excellent track record of distribution of these services and a solid commitment to best practices in management, monitoring and services.

- DEC 3

DEC 3 (Dynamic Enterprise Computing v3) is a service developed to provide safe and flexible cloud processing capacity to corporate users. By means of Computer Components, Consumer Elements that will determine the use of such components with added functionalities and supplementary Services that complete the solution, Customers may create a computing environment adequate for each of their essential applications. This way, customers can dispose and manage network, security and computation systems in a centralized and interrelated way, with complete independence of the physical components, the basic software and the architectures that support them. This concept helps the addition of new environments that cover the efficiency, technical and economic requirements from demanding applications.

DEC 3 is a Community Cloud Service, basically implemented with VMware tool. This tool provides a portal interface to clients to let them manage their environment with autonomy and in a simple and intuitive way, by using Vrealize Automation. Customers are able to manage their environment by creating virtual machines and limited to the resources hired to Cirion Technologies. Those limits are configured by Cirion Technologies operators for each client. Cirion Technologies performs capacity analysis from the computer resources of the cluster by using VCenter tool, from VMware,

Nevertheless, customers can delegate Cirion Technologies specialists the management of approved operational systems, databases and applications by hiring additional managed services.

Applicable Trust Services Criteria

The following Trust Services Criteria set forth in TSP section 100, “Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria, issued 2017) are covered by this report:

- **Security**

The security criterion refers to the protection of systems that use electronic information to process, transmit or transfer and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

- **Availability**

This criterion refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. The availability criterion does not address system functionality (the specific functions a system performs) or system usability (the ability of users to apply system functions to the performance of specific tasks or problems) but does address whether the system includes controls to support accessibility for operation, monitoring, and maintenance.

Relevant Aspects of Internal Controls

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process affected by an entity’s board of directors, management, and other personnel and consists of five interrelated components:

- **Control Environment** – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- **Risk Management** – The entity’s identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.
- **Information and Communication** – Surrounding these activities are information and communication systems. These enable the entity’s people to capture and exchange information needed to conduct and control its operations.
- **Monitoring** – The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.
- **Control Activities** – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary

to address risks to achievement of the entity's control objectives are effectively carried out.

This section briefly describes the components of Cirion Technologies' internal controls over the trust services principles and criteria of security and availability that may be relevant to customers.

Control environment

Cirion Technologies' organizational structure and, specifically, the Data Center's area organizational structure provides a framework for the planning, management and control of operations in which personnel and business functions are segregated into departments based on documented job descriptions. With this approach, the organization defines responsibilities as well as reporting and communication lines, and the employees focus on the tasks unique to their positions within the company. Sales (Sales), Operations (Network Operations) and Product (Product & Marketing) functions are organized under different VPs, who report to the company's President Regional.

The Data Center, Cloud & Security area (which belongs to the Product & Marketing area) is in charge of maintaining central infrastructure and carrying out the processes supporting the operation. In addition, there is a customer service area that participates in the first customer-service assurance level.

Global Security area is responsible for establish global policies of security for Cirion Technologies and the Data Center, Cloud and Security is responsible for procedures for maintain the security of every Data Center through monitoring activities and control activities on their internal system, with the objective to avoid external attacks or internal deficiencies.

Customer accounts are managed by an account executive belonging to the Sales vertical, who receives the assistance of sales support from the Data Center Product Line. There is also a Project Manager in the Data Center Product Line, who is in charge of implementing the service agreed upon with the customer.

Being part of GCL Group, Cirion Technologies is subject to the Foreign Corrupt Practices Act (the FCPA), which prohibits companies and their intermediaries from making improper payments to foreign officials for the purpose of obtaining or keeping business and/ or other benefits. The Company has policies and procedures designed to ensure that the company, its employees and agents comply with the FCPA.

The company has an employee recruitment policy in place that provides for the general conditions of the recruitment process. The recruitment process for each candidate is documented in the Success Factors tool, where it also possible to evaluate the performance of each employee and their goals.

The Company is committed to upholding the highest standards of ethics in relationships with customers, employees, shareholders and the business community. This commitment to ethical business practices is confirmed and contained in a Code of Conduct and Business Conduct policy, which includes counsel on ethical conduct and emphasizes its significance in all business activities.

The Code of Conduct must be read and accepted by all the employees joining the company.

The company's Code of Conduct has a specific section dealing with preventive measures to protect employees against conflicts of interest with the customers. A conflict of interest

is defined as any particular investment, interest, activity, association or service of Cirion Technologies employees or of any of their direct family members, which biases or seems to bias their judgment upon making decisions for the best benefit of Cirion Technologies or its customers.

The policies and procedures effective at the Company are applied both to Cirion Technologies' employees and contractors.

Cirion Technologies has a training calendar for all employees with mandatory courses about security, privacy among others to have updated the ethical knowledge of the company.

Vendor agreements include confidentiality commitments with Non-Disclosure Agreement clauses and the acceptance of the code of conduct.

The Board of Directors has Committees that have a number of independent Board members and where each Board and Committee member is qualified to serve in such capacity.

Risk assessment

Internal Audit

The Company's Internal Audit department, led by the Senior VP of Internal Audit and SOX Compliance, reports functionally to the Audit Committee of the Board of Directors and administratively to the Chief Financial Officer.

Internal Audit supports the Audit Committee and management through objective risk-based assurance and advisory services designed to add value and improve the operations of the Company. Internal Audit brings a systematic, disciplined approach to evaluating and recommending improvements to the risk management, control and governance processes, relating to, but not limited to operational, financial, compliance and information systems/technology.

Internal Audit has responsibility to:

- a) Develop a flexible annual audit plan using an appropriate risk-based methodology and submit the plan for review and approval by the Audit Committee.
- b) Regularly communicate to the Audit Committee information of the results of Internal Audit activities and progress on the annual plan.
- c) Issue audit reports to management summarizing significant audit observations and recommendations.
- d) Evaluate the action taken by management to address recommendations made by Internal Audit.
- e) Review the systems of internal control and risk management that management has implemented. This includes reviews of current and planned financial, management and operational systems, as well as steps taken to mitigate risks and impediments to the achievement of corporate objectives.

Risk Management

Data Center, Cloud & Security area, which supports local and regional directions, performs an annual audit plan for Data Center (Local and Regional audits). This plan must be reviewed by the correspondent Direction. Every audit plan has the evaluations and recommendations of improvements on processes, systems and infrastructure. This audit plan establishes the internal and external audits to be realized for each Data Center. Audits can be required from clients or from Cirion Technologies.

In addition to internal assessments, Cirion Technologies pursues various industry-recognized programs, including SOC 1 reports as well as this SOC 2 report, and ISO 27001 certification. The services and locations provided are ISO 27001 certified.

Every issue identified on the audits is documented on Cirion Technologies SharePoint to do a follow up and is reviewed in direction meetings to define a resolution plan. This is documented in the Cirion Technologies SharePoint and in the risk matrix, if necessary.

As part of the Risk Management and risk mitigation processes, Cirion Technologies has contracted insurance policies in place for operational risks such as earthquakes, flooding, storms and machine breakage.

Information & Communication

Cirion Technologies has a regulatory framework for its information system area, which consists of policies, procedures, configuration standards and technical documentation. Policies include the definition of basic standards for information protection, information security, user administration, security incidents administration and passwords, among others.

Based on the general standards defined, procedures were performed stating the steps for the implementation thereof. In addition, there are technical standards and procedures stating the values expected for operating systems, as well as the description of procedures stating the tasks to be performed to modify passwords or review logs, among others.

There are also formalized procedures to require and implement changes to programs supporting the company's transactions and the chart of account supporting book entries. Such procedures include defining the authorizations required in each case and the duties of each process participant.

The tools supporting Cirion Technologies operations require a username and a password. They validate if the user is authorized to perform an operation by verifying whether such user has a profile assigned for such purpose.

Cirion Technologies has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees; annual training programs tailored based on employee roles and responsibilities that may include Code of Conduct, Cirion Technologies Information Security Awareness, Business Continuity Management, Privacy Overview; regular management meetings for updates on business performance and other matters; and electronic means such as video conferencing, electronic mail messages, and the posting of information via the Cirion Technologies intranet on topics such as entity organization structure, process, organizational roles and responsibilities,

reporting of information security incidents and guidelines describing change management.

Services engagements are defined on Master Services Agreements to communicate Cirion Technologies responsibilities to clients.

Cirion Technologies performs an annual operational plan to determinate objectives for different areas as Sales, Delivery or Operative, among others. The plan is communicated to the areas involved to prepare or take actions to achieve the goals defined.

Monitoring

Monitoring activities are carried out through different methods. Management reviews the results of regulatory examinations, reports by Cirion Technologies' external auditor and client communications.

Internal monitoring is carried out by an administration committee and, specifically for the business line, by the data center management. Supervisory staff in general, monitors the performance, quality and controls as a normal part of its activities. Monitoring activities include reviewing the operating performance, quality control reviews and different reports that measure the results of processes involved in the data center operation.

The Data Center management, specifically the Executive VP, monthly analyzes financial and non-financial KPIs variations to study and examine business and operational performance and trends evolution. The analysis is performed for each branch.

Control Activities

Cirion Technologies has implemented procedures and controls to achieve service commitments and service requirements in accordance with its defined policies.

- ***Security Organization***
- ***Logical Access – User Access Management***
- ***Cybersecurity***
- ***Physical Access***
- ***System Monitoring and Incident Management***
- ***Change Management***
- ***Environmental Controls***
- ***Backups***
- ***Availability***

Complementary User Entity Controls (CUECS)

Housing/Colocation, Hosting and DEC3 Services security is a shared responsibility between the service provider and its customer. Cirion Technologies Housing/Colocation,

Hosting and DEC3 Infrastructure controls were designed with the assumption that certain controls would be implemented by user entities (or “customers”). Certain requirements can be met only if complementary user entity controls assumed in the design of Cirion Technologies Hosting, Hosting and DEC3 Infrastructure’s controls are suitably designed and operating effectively, along with related controls at Cirion Technologies Hosting, Hosting and DEC3 Infrastructure.

Impact of Covid-19 (Corona Virus)

In response to the global Covid-19 pandemic and at the direction of local, state and federal / governmental authorities in the jurisdictions in which we operate, Cirion Technologies implemented a work from home policy as of March 2020 for all non-essential employees and vendors. The architecture of the Cirion Technologies Hosting, Housing/Colocation and DEC3 Services System has been designed in a manner which enables Cirion Technologies to continue business as usual operations irrespective of the physical location of employees.

Cirion Technologies Hosting, Housing/Colocation and DEC3 Services System data center teams continue to perform and sustain standard operating procedures, as they relate to the controls tested in this audit. Due to the novel coronavirus, where required by local mandates, precautionary measures and limitations have been placed on the number of visitor staff and duration of visits at the data centers. In the event of a procedural impact or modification for the purposes of conforming to the constraints presented by Covid-19, Cirion Technologies Hosting, Housing and DEC3 Services System data center teams have initiated and executed any required approvals for such exceptions. Critical functions continue to operate.

Attachment B – Principal Service Commitments and System Requirements

Overview

Cirion Technologies designs its processes and procedures to meet its objectives for the Cirion Technologies Housing/Colocation, Hosting and DEC3 Services System. Those objectives are based on the service commitments that Cirion Technologies makes to user entities, the laws and regulations that govern the provision of the Cirion Technologies Housing/Colocation, Hosting and DEC 3 Services System, and the financial, operational and compliance requirements that Cirion Technologies has established for the services.

The Cirion Technologies Housing/Colocation, Hosting and DEC3 Services System are subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Cirion Technologies operates.

Security and Availability commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided on the Cirion Technologies website. Security, and Availability commitments are standardized and include, but are not limited to, the following:

- Security principle inherent to the fundamental design of the Cirion Technologies System is designed to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.
- Security principle inherent to the fundamental design of the Cirion Technologies System is designed to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.
- Availability principle inherent in the fundamental design of the Cirion Technologies System is designed to replicate critical system components at various locations and maintain the level of service to meet agreed SLAs.

Cirion Technologies establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Cirion Technologies' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Cirion Technologies Hosting, Housing/Colocation and DEC3 Services System.

As an Infrastructure as a Service (IaaS) System, the Cirion Technologies System is designed based on a shared responsibility model where both Cirion Technologies and the customers are responsible for aspects of security and availability. Details of the responsibilities of customers can be found on the Cirion Technologies website and in the Customer Agreement.









Multi User Report - ISAE 3402 - Cirion 2023 - SOC3


Relatório de auditoria final

2023-12-19


Criado em:	2023-12-19
Por:	Edney Kieger (edney.kieger.ext@ciriontechnologies.com)
Status:	Assinado
ID da transação:	CBJCHBCAABAARStyOauCCIlde8grexw-O-fNqXDHbzf0
Quantidade de documentos:	1
Contagem de páginas do documento:	14
Quantidade de arquivos de apoio:	0
Contagem de páginas dos arquivos de apoio:	0

Histórico de "Multi User Report - ISAE 3402 - Cirion 2023 - SOC 3"


-  Documento criado por Edney Kieger (edney.kieger.ext@ciriontechnologies.com)
2023-12-19 - 14:59:13 GMT
-  Documento enviado por email para gabriel.delcampo@ciriontechnologies.com para assinatura
2023-12-19 - 15:02:09 GMT
-  Documento enviado por email para pablo.dandois@ar.ey.com para assinatura
2023-12-19 - 15:02:09 GMT
-  Email visualizado por gabriel.delcampo@ciriontechnologies.com
2023-12-19 - 15:51:30 GMT
-  Contrato visualizado por gabriel.delcampo@ciriontechnologies.com
2023-12-19 - 15:51:32 GMT
-  O signatário gabriel.delcampo@ciriontechnologies.com inseriu o nome Gabriel del Campo ao assinar
2023-12-19 - 15:51:54 GMT
-  Documento assinado eletronicamente por Gabriel del Campo (gabriel.delcampo@ciriontechnologies.com)
Data da assinatura: 2023-12-19 - 15:51:56 GMT - Fonte da hora: servidor
-  Email visualizado por pablo.dandois@ar.ey.com
2023-12-19 - 18:12:33 GMT

 Contrato visualizado por pablo.dandois@ar.ey.com

2023-12-19 - 18:12:34 GMT

 O signatário pablo.dandois@ar.ey.com inseriu o nome Pablo Dandois ao assinar

2023-12-19 - 18:13:28 GMT

 Documento assinado eletronicamente por Pablo Dandois (pablo.dandois@ar.ey.com)

Data da assinatura: 2023-12-19 - 18:13:30 GMT - Fonte da hora: servidor

 Contrato finalizado.

2023-12-19 - 18:13:30 GMT