

SOCIEDAD DE EXPLOTACIÓN DE REDES ELECTRÓNICAS Y SERVICIOS S.A.

**Service Organization Control (SOC)
Report for SOCIEDAD DE EXPLOTACIÓN DE
REDES ELECTRÓNICAS Y SERVICIOS S.A. for
the period June 27th 2023 to June 26th 2024.**

Content

SECTION I.- INDEPENDENT SERVICE AUDITOR'S REPORT	4
1. Scope	4
2. Responsibilities of the service organization	4
3. Responsibilities of the Service Auditor	4
4. Limitations of controls in a service organization	5
5. Opinion	6
6. Description of the control tests	6
7. Targeted users and purpose	6
SECTION II.- WRITTEN MANAGEMENT STATEMENT ON SERVICE ORGANIZATION	8
Criteria description	8
SECTION III.- SYSTEM DESCRIPTION	11
SCOPE	11
RELEVANT ASPECTS OF GENERAL CONTROL	12
SECTION IV.- CONTROL TEST DESCRIPTION PROVIDED BY THE SERVICE AUDITOR	56
CONTROL OF OBJECTIVES AND TESTS CARRIED OUT	30

SECTION I:

INDEPENDENT SERVICE AUDITOR REPORT

SECTION I.- INDEPENDENT SERVICE AUDITOR'S REPORT

To: SOCIEDAD DE EXPLOTACIÓN DE REDES ELECTRÓNICAS Y SERVICIOS S.A. Service Organization

1. Scope

We have been examining to report on the description made by the SERES., of its Information security management system that supports the operation processes of B2B – B2C – B2G transactional services in SaaS mode, including electronic billing and tax reporting, as well as the preservation of the information and documents exchanged, with their corresponding signatures, seals and electronic certificate; SERES' national and international e-Invoice electronic invoicing services, including, either, e-Invoice Spain as an Electronic Invoice Exchange Platform, either e-Invoice Portugal as a Fatura Eletronica solution, either e-Invoice Mexico as PCCFDI of the SAT, either e-Invoice Colombia as a DIAN technology provider, either e-Invoice Peru as an Electronic Services Provider, either e-Invoice Argentina model AFIP, and either e-Invoice Ecuador SRI model; Tax reporting services: SII, SILICIE and TicketBAI; The S2P-O2C CONNECT[™] Electronic Document Exchange and Management Platform; The electronic signature service with full legal validity Contralia; Access point to the SERES Peppol network, during the period June 27th 2023 to June 26th 2024., and on the design and effective operation of the controls related to the control objectives indicated in the description, to provide reasonable assurance that service commitments and system requirements were met based on trusted service criteria relevant to security and availability (capacity, processing integrity, confidentiality, and privacy).

2. Responsibilities of the service organization

SERES service organization is responsible: for the preparation of the description and the statement attached in section II of the report, as well as for the completeness, accuracy and method of presentation of the description and affirmation; to provide the services covered by the alert, to indicate the control objectives; to design, implement and effectively apply controls to achieve the stated control objectives; and select the applicable trust service criteria and establish the related controls in the Description; and identify risks that threaten the fulfillment of service commitments and system requirements of the Service Organization.

3. Responsibilities of the Service Auditor

The Applus auditor's responsibility is to express an opinion on the SERES service organization's description and on the design and operation of controls relevant to the control objectives indicated in that description, based on our procedures. We conducted our order in accordance with International Standard on Assurance Engagements (ISAE) 3402 "Reports Providing Assurance on Controls in a Service Organization" issued by the International Standards on Auditing and Assurance Engagements Board. This standard requires us to follow ethical requirements and to plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and controls are properly designed and operating effectively, and Assurance Assignment Standard 3000: Assurance Assignments other than auditing or reviewing historical financial information, International Framework for Assurance Assignments and the concordance modifications of other International Standards for Assurance Assignments-NIEA.

These standards require that we comply with ethical requirements and that we plan and implement our procedures in order to obtain reasonable assurance that, in all material respects, the description is presented faithfully and the controls are properly designed and function effectively.

An assignment that provides a degree of assurance about the description, design, and operational effectiveness of controls in a service organization involves the application of procedures to obtain evidence about the information disclosed in the service organization's description of its system, and about the design and operational effectiveness of controls.

The procedures selected depend on the judgment of the service auditor, as well as an assessment of the risks that the description is not presented faithfully and that the controls are not properly designed or are not working effectively. Our procedures included testing the operating effectiveness of controls we considered necessary to provide reasonable assurance that the control objectives indicated in the description were achieved. A security engagement of this type also includes assessment of the overall presentation of the description, the adequacy of the objectives stated in the description, and the adequacy of the criteria detailed by the service organization and described in Section III.

Believe that the evidence we have obtained provides a sufficient and adequate basis for our opinion.

Examination of a description of a service organization's system and the adequacy of the design

and operational effectiveness of controls involves:

- Perform procedures to obtain evidence on the impartiality of the presentation of the Description and the suitability of the design and the operational effectiveness of the controls to achieve the related control objectives set out in the Description, based on the criterion in the management affirmation.
- Assess the risks that the Description is not presented adequately and that controls were not designed or functioned effectively to achieve the related control objectives set out in the Description.
- Test the operational effectiveness of such controls as management deems necessary to provide reasonable assurance that the related control objectives set out in the Description were achieved.
- Evaluate the overall presentation of the Description, the suitability of the control objectives established therein, and the suitability of the criteria specified by the service organization in its affirmation.

4. Limitations of controls in a service organization

The description made by the SERES service organization is prepared to meet the needs of its customers and auditors and it is possible, therefore, that it does not include every aspect of the system that your client may consider important in their particular environment. Likewise, due to their nature, it may happen that controls in a service organization do not prevent or detect all errors or omissions in the processing of transactions or in the preparation of reports on them. In addition, the forward-looking projection of any conclusions about the suitability of the design or the operational effectiveness of the controls is subject to the risk that the controls will become inadequate due to changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

5. Opinion

In our opinion, in all material aspects:

- (a) The description faithfully presents the SERES "Information security management system that supports the operation processes of B2B – B2C – B2G transactional services in SaaS mode, including electronic billing and tax reporting, as well as the preservation of the information and

documents exchanged, with their corresponding signatures, seals and electronic certificate; SERES' national and international e-Invoice electronic invoicing services, including, either, e-Invoice Spain as an Electronic Invoice Exchange Platform, either e-Invoice Portugal as a Fatura Eletronica solution, either e-Invoice Mexico as PCCFDI of the SAT, either e-Invoice Colombia as a DIAN technology provider, either e-Invoice Peru as an Electronic Services Provider, either e-Invoice Argentina model AFIP, and either e-Invoice Ecuador SRI model; Tax reporting services: SII, SILICIE and TicketBAI; The S2P-O2C CONNECT[™] Electronic Document Exchange and Management Platform; The electronic signature service with full legal validity Contralia; Access point to the SERES Peppol network" covering the activities of design, development, deployment, maintenance, enhancement, integration, support and marketing of software products for this service" as designed and implemented during the period June 27th 2023 to June 26th 2024;

(b) The controls related to the control objectives referred to in the description were properly designed during the period June 27th 2023 to June 26th 2024; and

(c) The controls that were tested, which were those necessary to provide reasonable assurance that the control objectives indicated in the description were achieved, functioned effectively during the period June 27th 2023 to June 26th 2024.

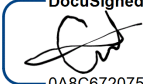
6. Description of the control tests

The specific controls that were tested and the nature, timing and results of such tests are detailed in Section IV of this report.

7. Targeted users and purpose

This report and the description of the Section IV control tests are intended only for clients who have used SERES ' Information security management system that supports the operation processes of B2B – B2C – B2G transactional services in SaaS mode, including electronic billing and tax reporting, as well as the preservation of the information and documents exchanged, with their corresponding signatures, seals and electronic certificate; SERES' national and international e-Invoice electronic invoicing services, including, either, e-Invoice Spain as an Electronic Invoice Exchange Platform, either e-Invoice Portugal as a Fatura Eletronica solution, either e-Invoice Mexico as PCCFDI of the SAT, either e-Invoice Colombia as a DIAN technology provider, either e-Invoice Peru as an Electronic Services Provider, either e-Invoice Argentina model AFIP, and either e-Invoice Ecuador SRI model; Tax reporting services: SII, SILICIE and

TicketBAI; The S2P-O2C CONNECT™ Electronic Document Exchange and Management Platform; The electronic signature service with full legal validity Contralia; Access point to the SERES Peppol network, service, and for its auditors, who have sufficient knowledge to take them into account, together with other information, including information on the controls applied by clients themselves, in assessing the risks of material misstatement in customers' financial statements.

DocuSigned by:

0A8C672075A7491...

Auditor: Karla Diaz Reyes
(B.U. Certification Systems)

SECTION II:

**WRITTEN MANAGEMENT STATEMENT ON
SERVICE ORGANIZATION BY SERES**

SECTION II.- WRITTEN MANAGEMENT STATEMENT ON SERVICE ORGANIZATION

We have prepared the description of the SERES system related to the characteristics of the Information security management system that supports the operation processes of B2B – B2C – B2G transactional services in SaaS mode, including electronic billing and tax reporting, as well as the preservation of the information and documents exchanged, with their corresponding signatures, seals and electronic certificate; SERES' national and international e-Invoice electronic invoicing services, including, either, e-Invoice Spain as an Electronic Invoice Exchange Platform, either e-Invoice Portugal as a Fatura Eletronica solution, either e-Invoice Mexico as PCCFDI of the SAT, either e-Invoice Colombia as a DIAN technology provider, either e-Invoice Peru as an Electronic Services Provider, either e-Invoice Argentina model AFIP, and either e-Invoice Ecuador SRI model; Tax reporting services: SII, SILICIE and TicketBAI; The S2P-O2C CONNECT[™] Electronic Document Exchange and Management Platform; The electronic signature service with full legal validity Contralia; Access point to the SERES Peppol network, service for customers who have used the SERES service during the period June 27th 2023 to June 26th 2024.

The description includes only the control objectives and related controls of SERES and excludes the control objectives and related controls of the subservice organization.

The description indicates that certain control objectives specified in the description can only be achieved if the complementary user entity controls assumed in the design of the SERES controls are properly designed and functioning effectively, together with those related to the controls in the service organization. The description does not extend to the controls of the user entities.

The description is intended to provide reporting users with information about our system that may be useful in assessing the risks arising from interactions with the SERES system, in particular information about the system controls that SERES has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the criteria of trust relevant to security and availability.

Criteria description

We confirm, to the best of our knowledge and belief, that:

1. The description fairly presents the SERES system that was made available to the entity that is a user of the system for part or all of the period June 27th 2023 to June 26th 2024 to process their transactions. The criteria we used to make this statement were that the Description:

a). Presents how the system made available to the user entity to process relevant transactions was designed and implemented, including, if applicable:

- The types of services provided, including, as appropriate, the types of transactions processed.
- The procedures, both automated and manual, by which such services are provided, including, as appropriate, the procedures by which they are initiated, authorized, recorded, processed, corrected as necessary and transferred to reports and other information prepared for entities using the system.
- The information used in the execution of procedures, including, where applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing and reporting transactions; this includes correcting incorrect information and how the information is transferred to reports and other information prepared for the user entity.
- How the system captures and addresses significant events and conditions.
- The process used to prepare reports or other information provided to the system user entity.
- Services performed by a subservice's organization, if any.
- The specified control objectives and controls designed to achieve those objectives, including, as appropriate, the complementary controls of the user entity assumed in the design of the controls of the service organization.
- Other aspects of our control environment, the risk assessment process, information, and communications (including related business processes), control activities and monitoring activities that are relevant to the services provided.

b). The description includes relevant details of changes to the SERES system during the period covered by the description when the description covers a period.

c). The Description does not omit or distort information relevant to the service organization's system, while acknowledging that the Description is prepared to meet the common needs of the system customers.

2. Controls related to the control objectives set out in the Description were properly designed and operated throughout the period June 27th 2023 to June 26th 2024 to achieve those control objectives. The criteria we used to make this statement were that:

- The risks that threaten the achievement of the control objectives set out in the Description have been identified by SERES.
- The controls identified in the Description would provide, if they function as described, reasonable assurance that those risks would not prevent the control objectives set out in the Description from being achieved.
- Controls were applied systematically as designed, including whether manual controls were applied by persons who have the appropriate competence and authority.

Luis Lopez Martinez
(CSO – Chief Security Officer)

SECTION III:

SERES DESCRIPTION OF THE SYSTEM

SECTION III.- SYSTEM DESCRIPTION

This report describes the control structure of SERES, part of the French group Dicaposte, specializes in the digitalization of business processes and the secure electronic exchange of documents. As a trusted third party, we offer relationship solutions B2B, B2G and B2C, focusing on digital transformation through comprehensive services that include solutions development, global support and change management. Its objective is to improve the efficiency and security in business and data communication.in relation to its Information security management system that supports the operation processes of B2B – B2C – B2G transactional services in SaaS mode, including electronic billing and tax reporting, as well as the preservation of the information and documents exchanged, with their corresponding signatures, seals and electronic certificate; SERES' national and international e-Invoice electronic invoicing services, including, either, e-Invoice Spain as an Electronic Invoice Exchange Platform, either e-Invoice Portugal as a Fatura Eletronica solution, either e-Invoice Mexico as PCCFDI of the SAT, either e-Invoice Colombia as a DIAN technology provider, either e-Invoice Peru as an Electronic Services Provider, either e-Invoice Argentina model AFIP, and either e-Invoice Ecuador SRI model; Tax reporting services: SII, SILICIE and TicketBAI; The S2P-O2C CONNECT[™] Electronic Document Exchange and Management Platform; The electronic signature service with full legal validity Contralia; Access point to the SERES Peppol network, from the period June 27th 2023 to June 26th 2024. This report, which includes the description of the controls in this Section, is intended solely for the information and use of the Company, the entities that use the Platform for the entire Specified Period, and the independent auditors of such user entities. This report should not be used by anyone other than these specified parts.

The Information system that supports the service is designed to meet security, privacy, and compliance requirements.

SERES has an adequate system to provide confidentiality, integrity and availability of customer data. It also provides transparent accountability to enable customers and their agents to track service management.

SERES has selected Oracle Cloud Infrastructure (OCI) as its main cloud infrastructure provider, responsible for the infrastructure that supports services in the 'Central Germany (Frankfurt)'

region of this provider, which guarantees the security management of the information in the provided services.

Any supplier or partner that may have an influence on the confidentiality, integrity, availability, traceability, and authenticity of the information included in the scope of the Information Security Management System (ISMS) of ENS, hereinafter Technological Provider(s); must be selected and evaluated in accordance with the "Information Security Policy in Relations with Suppliers" and the procedures established by SERES to guarantee information security.

SERES has defined the specific defense lines for each one of the services including the connection elements from the exterior and the access points for the system.

RELEVANT ASPECTS OF GENERAL CONTROL

SERES has implemented several controls within the organization, such as policies, procedures, methods and organizational structure of the organization, which are properly communicated through the organization, properly owned, managed and supported, focused on continual iteration and improved and supported by a policy framework and structure.

The trust services categories that are in scope for the purpose of this report are defined in the following sections:

1.1 Control environment

The 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. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.

SERES control environment is focused on establishing, enhancing and supervising the effectiveness of specific controls:

- Integrity and ethical values
- Commitment to competence

- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and practices

1.2 Risk Assessment

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives and thus risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.

SERES has placed into operation various processes to identify and manage risks that could affect your clients.

1.3 Information and Communication

Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems deal not only with internally generated data, but also information about external events, activities and conditions necessary for informed business decision making and external reporting.

Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel receive a clear message from top management that control responsibilities must be taken seriously. They understand their own role in the internal control system, as well as how individual activities relate to the work of others. They have a means of communicating significant information upstream. There also needs to be effective communication with external parties.

1.4 Control Activities

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and

in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliation, reviews of operating performance, security of assets and segregation of duties.

1.5 Monitoring and Internal Auditing

Internal control systems are monitored by a process that assesses the performance over time. It is accomplished through both ongoing monitoring activities as well as periodic, separate evaluations. Monitoring controls operate at the entity level as well as at the process level.

SERES monitors the quality and security of internal control performance regarding ISO 27001, ENS, ISO 9001, Accounts audit and Data Protection controls.

As a result of the aforementioned control monitoring, reports with the details of the arisen issues and their solution are periodically done.

The SERES Information security management system that supports the operation processes of B2B – B2C – B2G transactional services in SaaS mode, including electronic billing and tax reporting, as well as the preservation of the information and documents exchanged, with their corresponding signatures, seals and electronic certificate; SERES' national and international e-Invoice electronic invoicing services, including, either, e-Invoice Spain as an Electronic Invoice Exchange Platform, either e-Invoice Portugal as a Fatura Eletronica solution, either e-Invoice Mexico as PCCFDI of the SAT, either e-Invoice Colombia as a DIAN technology provider, either e-Invoice Peru as an Electronic Services Provider, either e-Invoice Argentina model AFIP, and either e-Invoice Ecuador SRI model; Tax reporting services: SII, SILICIE and TicketBAI; The S2P-O2C CONNECT[™] Electronic Document Exchange and Management Platform; The electronic signature service with full legal validity Contralia; Access point to the SERES Peppol network, service offers its clients is made up of generic processes attending to the business requirements and the technical means necessary for these to be carried out. These processes constitute the Information Management System for this service and comprise a set of Control Objectives safeguarding the service quality and the protection and safety of information.

DETAILED DESCRIPTION OF THE CONTROL ENVIRONMENT

The objectives of SERES` s control environment is to set the tone for the organization` s internal control. Integrity, ethical values, and competence are key elements of SERES control environment.

The employees are required to acknowledge the Code of Conduct. The Human Resources (HR) Operations team is involved in reviewing and monitoring that these policies and agreements are acknowledged, and that background screening is followed through in a timely manner. Employees and contractors with access to systems are asked to re-acknowledge the Code of Conduct in a periodic basis.

SERES stands out for its commitment to the professional development of its employees. The company firmly believes that every individual has the potential to achieve great things and perform exceptional work when given the right support. To ensure the constant growth and updating of its collaborators, SERES offers a wide range of training opportunities such as security awareness, technical formation, ethics and Culture awareness, professional development, anticorruption statement, adherence to human rights, among others.

SERES organizational structure is managed by a security committee as follows:

- Service Manager
- Information Manager
- Systems Manager
- Security Mnagaer
- Data Protection Officer

To maintain strong corporate governance practices, SERES' Board of Directors and its subcommittees convene in a periodic basis. These meetings focus on reviewing committee charters and overall corporate governance policies. These charters outline the roles and responsibilities of each committee, member qualifications, meeting frequency, and key discussion topics. Detailed minutes are kept for each annual meeting, recording participants and the date. Additionally, the process for identifying and evaluating potential Board of Directors candidates is clearly defined within the Nominating and Governance Committee charter.

At SERES, we prioritize finding talented individuals who possess relevant experience, a strong educational background, and a dedication to ethical conduct. To achieve this, we leverage our applicant tracking system to gather interview feedback for all onsite candidates. This ensures everyone involved in hiring, from recruiters to hiring managers and HR, has access to a comprehensive candidate profile and valuable interview insights. No offer is extended without at least one interview review documented in Lever before the start date.

Job descriptions clearly outline roles and responsibilities, accessible both in advertisements and within Lever. Background checks are conducted for all full-time hires and results are reviewed. For agency-placed contractors, background checks are the responsibility of the agency itself, with SERES maintaining a contract to ensure timely completion and proper assessment.

SERES takes data security and confidentiality seriously. New hires are thoroughly informed and acknowledge our company's policies for protecting assets. The HR Operations team delivers this information during onboarding, and all employees and contractors are required to sign a Confidential Information. A periodic review ensures signatures are obtained before each new employee's start date.

At SRRES, we believe in fostering a culture of continuous development. In the first months of incorporation, people leaders (managers) conduct performance check-ins with their team members as a performance evaluation. After feedback is gathered, managers provide performance ratings and assess each team member's relative contribution.

DETAILED DESCRIPTION OF THE COMMUNICATION AND INFORMATION

SERES maintains a Policy Management Program to help ensure that policies and procedures are properly communicated throughout the organization, properly owned, managed, and supported, clearly outlining business objectives, showing commitment to meeting regulatory obligations, focused on continual iteration and improvement, supported by the Policy Framework and Structure.

At SERES we understand that effective policies are vital for managing risk. Each policy has a Trust service criteria, Related controls and test of controls related to the Security, Availability and Confidentiality Categories by Applus+ 19

designated owner responsible for overseeing the specific risk outlined within the policy's objective. To ensure our policies remain relevant and effectively manage risk, we conduct annual reviews to assess their alignment with SERES` s risk tolerance.

SERES defines policies, standards, guidelines, and procedures, and each document maintained by SERES is classified into one of the categories defined.

At SERES we prioritize keeping our customers informed and empowered. We achieve this through a comprehensive communication strategy that encompasses a variety of channels and topics. We provide readily accessible policies and guidelines on our website, ensuring our customers understand their responsibilities and how we operate. We promptly communicate any changes related to security measures, keeping our customers informed of potential risks and necessary actions. We transparently communicate product updates, feature changes, and upcoming developments, allowing customers to stay ahead of the curve. For critical situations, we utilize product alerts to notify customers of potential issues and recommended solutions. We openly communicate any changes to our commitments regarding service availability and data confidentiality.

We understand the importance of open communication. That's why we offer multiple channels for both customers and internal users to report any issues. Security vulnerabilities and security incidents are a top priority. We encourage to report any vulnerabilities or incidents that are discovered using our established processes.

DETAILED DESCRIPTION OF THE RISK ASSESMENT

At SERES we understand that achieving our ambitious business objectives requires a proactive approach to risk management. That's why we've implemented a robust Enterprise Risk Management process. By proactively managing risk, SERES safeguards our path to success and ensures we can continue delivering exceptional value to our customers.

This comprehensive framework allows us to:

- Identify the Landscape: We begin by meticulously analyzing both internal and external factors that could impact our company's goals.
- Evaluate Potential Risks: Once the landscape is clear, we thoroughly assess potential risks that could hinder our progress.
- Develop Mitigation Strategies: For each identified risk, we strategically develop mitigation plans to minimize potential disruptions.
- Clear Communication: The outcomes of our risk assessments and mitigation strategies are openly communicated across the organization.
- Continuous Monitoring: We don't stop at planning. We continuously monitor the execution of our risk strategies and remain vigilant to any changes in the business environment that could introduce new risks.

Our Enterprise Risk Management framework goes beyond individual functions or departments. We assess risks based on their impact on the entire organization, not just isolated areas. While specific considerations may exist for a particular product or service, these are always evaluated in the context of their potential impact on SERES as a whole. This principle applies not only to the analysis of risks but also to their final evaluation.

Also, at SERES, we take a proactive stance against fraud. The Head of Risk and Compliance spearheads an annual fraud risk assessment to identify and mitigate potential vulnerabilities.

To ensure objectivity, an independent third-party company analyzes the combined survey data and external threat assessment. Their report identifies and prioritizes potential areas of risk within SERES.

The Head of Risk and Compliance then reviews these identified risks and recommendations. Action plans are developed and implemented on a case-by-case basis to address any vulnerabilities. If necessary, these recommendations are also incorporated into SERES' broader Enterprise Risk Management framework.

The results of the annual fraud risk assessment are included within the overall enterprise risk assessment report. This comprehensive report is communicated to both the board and executive-level managers, fostering transparency and ensuring informed decision-making across leadership

At SERES, we understand the importance of thorough vendor evaluation. To mitigate potential risks, high-risk vendors undergo a comprehensive risk assessment and review process as part of onboarding.

This multi-layered approach involves internal Subject Matter Experts (SMEs) from across various departments. They meticulously evaluate the vendor's control environment and overall security posture. This evaluation considers information from several sources:

- Vendor Questionnaires: Detailed questionnaires provide insights into the vendor's internal practices and risk management strategies.
- Compliance Reporting: Audit Reports such as SOC 2, ISO 27001, ENS, among others attestations offer valuable evidence of the vendor's adherence to industry security standards.
- Vendor Policies: A review of the vendor's policies ensures alignment with SERES' own security, confidentiality, and availability commitments.

Before any partnership commences, SERES establishes clear expectations through vendor agreements. These agreements outline terms and conditions, along with specific commitments related to security, confidentiality, and availability. Only after a successful risk assessment and a signed agreement does a vendor relationship proceed.

By implementing this rigorous onboarding process, SERES safeguards its business from potential security threats and ensures trusted partnerships with its vendors.

DETAILED DESCRIPTION OF THE MONITORING ACTIVITIES

Information security metrics are crucial tools for monitoring an organization's systems and safeguarding sensitive data. These metrics enable SERES to quantify and evaluate the effectiveness of their security controls, identify areas of potential risk, and take proactive measures to mitigate threats

By implementing an information security metrics program, SERES can reap a multitude of benefits, including:

Trust service criteria, Related controls and test of controls related to the Security, Availability and Confidentiality Categories by Applus+ 22

- Enhanced Security Posture Visibility: Metrics provide a clear and objective view of an SERES` s information security posture, allowing security professionals to swiftly identify and address weaknesses.
- Prioritized Security Initiatives: Metrics can be utilized to pinpoint areas of highest risk, enabling SERES to allocate their security resources more effectively.
- Demonstrated Compliance: Many information security regulations mandate that organizations implement a security metrics program. Metrics are used to demonstrate compliance with these regulations.
- Improved Decision-Making: Metrics provide valuable insights that can be used to make informed decisions regarding information security.

At SERES, we prioritize the security of our systems and data. A core element of this commitment is our comprehensive vulnerability management process. By proactively tracking, prioritizing, and resolving vulnerabilities, SERES fosters a secure environment for its users and data.

Our organization utilizes the following tools for scanning the internal and external-facing network, as well as configurations:

- Endpoint XDR (extended detection and response)
- A unified cloud security platform for cloud security that includes prevention, active detection and response
- Examinations of our Cloud Infrastructure resources for security weaknesses related to configuration and monitoring of operators and users for risky activities
- Regular Pentesting exercises.

Ongoing workstation asset management, security patch deployment, password protection, screensaver and screen lock settings, and drive encryption auditing are done using policies deployed through the AD.

SERES employs a robust security strategy to protect against email-borne threats.

- **Perimeter Defense:** Serves as our first line of defense, filtering out malicious emails at the network perimeter before they ever reach your inbox. This proactive approach minimizes the risk of malware infection.
- **Empowering Users:** We believe in a layered security approach. In addition to technical safeguards, we equip our employees with the knowledge to identify potential threats. Through annual security training programs, we educate staff on a variety of security risks, including those associated with email phishing attempts. These training sessions empower employees to play a vital role in maintaining a secure email environment.

Customer data is encrypted at rest, and external connections to the Systems are encrypted in transit via the secured defined protocols. SERES monitors the certificate authority issued TLS certificates and renews them prior to expiry.

At SERES, we are dedicated to maintaining strong internal controls and adhering to industry standards. Our commitment to compliance is achieved through a two-pronged approach; Our Internal Audit team conducts comprehensive audits on a regular basis, focusing on key areas such as operational audits, ISO audits, account audits, NIS audits, SOC audits, among others.

DETAILED DESCRIPTION OF THE CONTROL ACTIVITIES

The user creation process is a critical component of SERES` s security posture. It ensures that only authorized individuals are granted access to sensitive systems and data. A well-defined user creation process helps to mitigate the risk of unauthorized access, data breaches, and other security incidents.

The user creation process begins with a request from a manager or supervisor. The request should specify the user's name, role, and the systems and data they need to access in order to have the complete information.

The IT department or a designated administrator creates the user account in the organization's identity and access management system. This involves setting up a username, password, and assigning appropriate access permissions.

Once the account is created, the necessary access permissions are granted to the user. This

may involve adding the user to specific groups, granting them access to particular applications, or assigning them roles with defined privileges.

Before granting full access, the user's account and access permissions should be reviewed and approved by a manager or supervisor. This helps to ensure that access is granted only to those who legitimately need it.

New users should be provided with onboarding and training to familiarize them with the organization's security policies, procedures, and best practices. This helps to minimize the risk of accidental security breaches. Access permissions are reviewed and updated regularly to reflect changes in the user's role or responsibilities. Additionally, terminated users' access should be revoked promptly to prevent unauthorized access.

Passwords are an important part of SERES` s efforts to protect its technology systems and information assets by helping to ensure that only approved individuals can access these systems and assets, that why the strong Password Policies are implemented to enforce strong password policies to protect against password cracking and other attacks. Multi-Factor Authentication (MFA) adds an extra layer of security to user authentication; Least Privilege Principle guarantees that users only the minimum access permissions they need to perform their job duties as well as the regular security audits to identify and address any vulnerabilities in the user creation process.

At SERES we prioritize maintaining a seamless user experience. To achieve this, we have implemented a robust, company-wide incident management process. This process aligns with the SERES Incident Management Standard, ensuring a structured and effective approach to resolving any service interruptions or security concerns.

Our incident management process is laser-focused on minimizing downtime, service degradation, or security risks for both our customers and internal users. Every step taken to address an incident is meticulously documented within an Incident Management System using a dedicated incident ticket. This allows for clear communication, efficient problem-solving, and thorough post-incident analysis.

A good change management system is all about effectively guiding SERES through transitions,

whether it's implementing a new software program, restructuring departments, or updating security protocols.

Providing an structured framework provides a clear, step-by-step process for planning, implementing, and monitoring changes. This framework should be adaptable to different types and sizes of changes, as well as identifying the potential risks, develop mitigation strategies, and monitor for any issues that may arise.

Capacity management is performed on an ongoing basis by all products. The infrastructure and systems that make up each product are continuously monitored for utilization levels and adjusted accordingly.

A disaster recovery policy is in place and is reviewed on an annual basis by the disaster recovery steering committee. Procedures for disaster recovery execution are defined, reviewed, tested, and in place. The policy describes, at a high level, the purpose, objectives, scope, critical dependencies, recovery time objective/recovery point objective (RTO/RPO), and roles and responsibilities.

Disaster recovery tests are performed on a regular basis and in a simulated environment. Tabletop exercises are also performed to help disaster response teams walk through various scenarios of incidents. After disaster recovery tests are performed, outputs of the tests are captured, analyzed, and discussed to determine the scope of the next steps for continuous improvement of the tests. The improvement efforts are captured within engineering tickets and followed through as appropriate

SECTION IV:

CONTROL TEST DESCRIPTION PROVIDED BY THE SERVICE AUDITOR APPLUS+

SECTION IV.- CONTROL TEST DESCRIPTION PROVIDED BY THE SERVICE AUDITOR

A description of the tests carried out by Applus+. to determine whether SERES controls work effectively enough to achieve specified control objectives. Applus+ determined the nature, time and extent of the tests carried out.

Our review was conducted in accordance with Statement on Standards for Attestation Commitments No. 18 (SSAE 18), established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Commitments 3402, Assurance Reports on Controls in a Service Organization, published by the International Board of Auditing and Assurance Standards.

TYPES AND DESCRIPTIONS OF OPERATIONAL EFFECTIVENESS TESTS

Applus+ performed a variety of tests related to the controls listed in this section throughout the period June 27th 2023 to June 26th 2024 and applied to the controls relating to the control objectives specified by SERES.

The tests performed are described below:

Type	Description
Consultation	Consult relevant staff, including, but not limited to: <ul style="list-style-type: none"> • Knowledge and additional information about the policy or procedure; and • Corroborate evidence of the policy or procedure. As queries were performed for substantially all controls, the test was not included individually for each control shown in the accompanying matrices
Walkthrough	Explanation and demonstration of provided

	process description or documentation (including control activities) by responsible staff personnel
Inspection	<p>Inspected documents and records indicating the performance of controls. This test included, among other things:</p> <ul style="list-style-type: none"> • Examinations of the documentation and authorizations to verify the processed procedures; • Examination of documents or records for evidence of performance, such as the existence of initials or signatures; and • Inspection of system documentation, such as operations manuals, flowcharts, and job descriptions.
Observation	The application or existence of specific controls represented was observed.

CONTROL OF OBJECTIVES AND TESTS CARRIED OUT

Control	Description of controls	Requested Evidence / Test of Controls (for the sample)	Test Results
CONTROL ENVIRONMENT			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	<ul style="list-style-type: none"> -Background check verifications -Confidential agreements -Code of conduct -Evaluation of the competences of employees 	No exceptions have been observed
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	<ul style="list-style-type: none"> -Security committee -Roles and Responsibilities -Committee meeting minutes 	No exceptions have been observed
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	<ul style="list-style-type: none"> -Information security Policy -Crisis Committee -Communication with authorities -Job descriptions of employees 	No exceptions have been observed
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	<ul style="list-style-type: none"> -Job descriptions of employees -Job offers and approvals -Performance 	No exceptions have been observed

		evaluation -Training plan and training tools -Training evaluations	
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	-Job descriptions -Code of conduct -Performance evaluation -Training plan and training tools -Training evaluations	No exceptions have been observed
COMMUNICATION AND INFORMATION			
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	-Internal and external vulnerability scans -Remediations actions for vulnerabilities -Log management tool -Internal audits documentations and test results	No exceptions have been observed
C2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	-Website and intranet with the defined boundaries -System changes -Objectives and strategic plans -Incident channel communication for external and internal interested parties -Security Policy -Signature of the security responsibilities	No exceptions have been observed

		by employees	
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	<ul style="list-style-type: none"> -Privacy policy -Providers communication portal -Contracts of some critical vendors -Security agreements with providers -Communication of changes -Objectives communication with external and internal interested parties 	No exceptions have been observed
RISK ASSESSMENT			
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	<ul style="list-style-type: none"> -Risk assessment methodology and risk assessment iteration for the audit period -Risks documentation -Treatment Action Plans and follow up 	No exceptions have been observed
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	<ul style="list-style-type: none"> -Disaster recovery policy -Risk assessment -Risks documentation -Treatment Action Plans and follow up 	No exceptions have been observed
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the	<ul style="list-style-type: none"> -Risk assessment -Risk associated with frauds 	No exceptions have been

	achievement of objectives.	-Treatment Action Plans and follow up	observed
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	-Penetration test report -Tickets for the follow up of the vulnerabilities detections	No exceptions have been observed
MONITORING ACTIVITIES			
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	-Vulnerability scan configurations -Remediation documentation -Penetration tests report -Tickets for the follow up of the vulnerabilities detections	No exceptions have been observed
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	-Internal audit documentation	No exceptions have been observed
CONTROL ACTIVITIES			
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	-Risk mitigation strategies -Risk assessment documentation -Business impact analysis for the services	No exceptions have been observed

		-Process map	
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives	-Security reviews in a periodic basis	No exceptions have been observed
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action	<ul style="list-style-type: none"> -Policies for the development, acquisition, implementation changes and maintenance of security systems -Classification policy -Accessibility of the policies -Access control procedure -Users account management -Information security policies -Backup and recovery procedures -Vulnerability management -Incident management -Sample of security events and incidents -Vendors and providers evaluation and management 	No exceptions have been observed
LOGICAL AND PHYSICAL ACCESS CONTROLS			

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	<ul style="list-style-type: none"> -System´s configurations -Authentication methodologies -Remote login -Multiple factor authentication -VPN remote connections -Active Directory -Data store configurations -Accesses monitorization - 	No exceptions have been observed
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	<ul style="list-style-type: none"> -Admin users management -Access requests tickets -Active Directory groups assignments Active directory group policies -Automatic alerts configurations in the systems -Access reviews and approval documentation 	No exceptions have been observed
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets	<ul style="list-style-type: none"> -Admin users management -Access requests tickets -Active Directory groups 	No exceptions have been observed

	based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	<p>assignments</p> <p>Active directory group policies</p> <p>-Automatic alerts configurations in the systems</p> <p>-Access reviews and approval documentation</p>	
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	<p>-Data centers security</p> <p>-Physical entry controls</p> <p>-Working in secure areas</p> <p>-Return of assets</p>	No exceptions have been observed
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	<p>-Asset inventory</p> <p>-Secure disposal</p> <p>-Secure guard of assets</p> <p>-Return of assets</p> <p>-Physical entry controls</p>	No exceptions have been observed
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	<p>-Systems configuration</p> <p>-IT asset management system</p> <p>-Multi factor authentication systems</p>	No exceptions have been observed
CC6.7	The entity restricts the	-IT asses management	No

	transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	system	exceptions have been observed
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	-NAC scan -Antimalware software configurations	No exceptions have been observed
SYSTEMS OPERATIONS			
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities	-Monitorization of assets and connections system -Internal and external vulnerability scans -Remediation documentation	No exceptions have been observed
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	-Monitoring tools -Penetration tests -Log management tools configurations	No exceptions have been observed

CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	-Incident management -Sample of security events and incidents -Tickets for remediation -Security gaps communications	No exceptions have been observed
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	-Incident management	No exceptions have been observed
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	-Disaster recovery policy -Incident management -Sample of security events and incidents -Incident response plan	No exceptions have been observed
CHANGE MANAGEMENT			
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	-Systems configurations -Alerts configuration -Inspected scanning configurations	No exceptions have been observed
RISK MITIGATION			
CC9.1	CC9.1: The entity identifies, selects, and develops risk	-Disaster recovery plan -Incident management	No exceptions

	mitigation activities for risks arising from potential business disruptions.	-Response plan -Tests results	have been observed
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	-Contracts with critical vendors -Agreements and evaluations	No exceptions have been observed
ADDITIONAL CRITERIA FOR AVAILABILITY			
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	-Monitoring tools	No exceptions have been observed
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	-Backup configurations -Restoration tests -Alert configuration -Disaster recovery plan -Recovery procedures -Replications	No exceptions have been observed
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	-Cloud disaster recovery plan -Backup and recovery procedures -	No exceptions have been observed
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			

C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	-Acquisition, development and maintenance policy -Test data, production data -Classification policy -Development policy -Contracts with critical vendors	No exceptions have been observed
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	-Retention periods of information -Storage data configurations	No exceptions have been observed
ADDITIONAL CRITERIA FOR PROCESS INTEGRITY			
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.	-Data process procedure	No exceptions have been observed
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	-Acquisition security requirements	No exceptions have been observed
PI1.3	The entity implements policies and procedures over system	-Acquisition security requirements	No exceptions

	processing to result in products, services, and reporting to meet the entity's objectives.		have been observed
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.	-Acquisition security requirements -Security policies with providers	No exceptions have been observed
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives	-Assets guards	No exceptions have been observed
ADDITIONAL CIRTERIA FOR PRIVACY			
P1.1	The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P2.1	The entity communicates choices available regarding the collection, use, retention,	-Treatment Activities registry (RAT)	No exceptions have been

	disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.		observed
P3.1	Personal information is collected consistent with the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to	-Treatment Activities registry (RAT)	No exceptions have been observed

	meet the entity's objectives related to privacy.		
P4.1	The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P4.2	The entity retains personal information consistent with the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P4.3	The entity securely disposes of personal information to meet the entity's objectives related to privacy	-Treatment Activities registry (RAT) -Removal, access requests to personal information	No exceptions have been observed
P5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P5.2	The entity corrects, amends, or appends personal information based on information provided	-Treatment Activities registry (RAT)	No exceptions have been

	by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.		observed
P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P6.2	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P6.3	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy	-Treatment Activities registry (RAT)	No exceptions have been observed
P6.4	The entity obtains privacy	-Treatment Activities	No

	commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	registry (RAT)	exceptions have been observed
P6.5	The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P6.6	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data	-Treatment Activities registry (RAT)	No exceptions have been observed

	subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.		
P7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	-Treatment Activities registry (RAT)	No exceptions have been observed
P8.1	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.	-Treatment Activities registry (RAT)	No exceptions have been observed

FIRMA DEL INFORME

Applus+Certification (LGAI TECHNOLOGICAL CENTER,
S.A.)

www.appluscertification.com

Fecha inicial del informe: 26/06/2024

Fecha de la última modificación del informe: **Cambios realizados:**

Número de edición: 1

El Representante de la organización

Firma:

Nombre D/D^a Luis Lopez (CSO)

El equipo auditor

Firma:

DocuSigned by:

0A8C672075A7491...

Nombre D/D^a [Karla Diaz Reyes]
B.U. CERTIFICACIÓN DE SISTEMAS