ASSESSMENT RISK AND CONTROLS MATRIX																		
1st STEP				2nd STEP						3rd STEP								4th S
Company/Segment/Period				Risk Identification/Assessment						Identification/evaluation of controls								Risk
ID	Area/Process	Subprocess	Description/Activity	Description/Risk	Category / Risk	Probability	Impact	Gross Risk	Observations	Control	Description	Objective	Nature	Kind	Enhancement/Frequency	Evaluation
1.1.1	Systems Database	Import Database	Import Database from the CASEID and RMS systems to transfer this data to carry out behavioral analysis of the industry, with treatment of historics.dat.zaw time.	Breach of contractual clauses, modification of agreed conditions, fees, deadlines, guarantees without the consent of the parties involved.	Inappropriate Practices (Customers, Products and Services)	Average	High	High	Create a document to be aware of the limits to people (confidentiality agreement), DPO participating in the process	1	Confidentiality agreement	To make people aware of their limits	Preventive	Manual	On-Demand	Satisfactory
										2	Training and Reinforcement of awareness for the project team	Ensure that everyone knows the project's data confidentiality rules	Preventive	Manual	On-Demand	Satisfactory
1.1.2	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID and RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to carry out behavioral analysis of the industry	System Failures related to equipment, software, applications, or communication infrastructure.	System Failures	Low	Low	Low	The risk is dependent on the configuration use Databricks, Azure cloud, meets 27k security requirements, get evidence. Create a specific instance for this project to implement the necessary controls. This is a list of requirements for configuration level https://azure.microsoft.com/pt-br/explore/trusted-cloud/	3	Create Specific Cloud Instance	segregate the data processing environment from the other SBNAI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										4	Databricks Security Controls	Evidence of best practices and avoid ctrl misconfiguration	Preventive	Automatic	Daily (multiple times)	Satisfactory
1.1.3	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID and RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to carry out behavioral analysis of the industry	Parameterization of the databricks tool links	Process Execution and Management	High	High	High	Parameterization with be performed by a Microsoft specialist. User cannot change the defined parameters. There is evidence of the competence of the company that will parameterize (PM) must present the product certifications. Parameterization is carried out by it funds, using the standards of best practices and safety standards of SBNAI SoD - Who uses it does not configure	5	Segregation of Duties	Do not allow the user to change the segregation of settings	Preventive	Manual	On-demand	Regular
										6	Expert Performed Databricks Setup	Ensure the accuracy of settings	Preventive	Manual	On-demand	Satisfactory
										7	Expert Performed Databricks Setup	Ensure assertiveness of configurations confidentiality and handling of project data	Preventive	Manual	On-demand	Regular
										7	Training and awareness reinforcement for project team	Ensure that everyone knows the project's data confidentiality rules	Preventive	Manual	On-demand	Satisfactory
1.1.4	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID and RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to carry out behavioral analysis of the industry	Failure of procedures and/or application of internationalized standards (Absence of control tools to monitor the execution of internal and external standards and procedures required by regulatory bodies)	Process Execution and Management	High	High	High	Implementation of audit, add to the quarterly cycle. Include PAM tool to monitor.	8	Audit	Check level of adherence to policies, standards, etc.	Detective	Manual	Monthly	Satisfactory
										9	Tool to PAM	Monitor Privileged Access	Preventive	Automatic	Daily (multiple times)	Strong
1.1.5	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID and RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Data import - Absence of documentation supporting records and entries made (Make entries if the document supports justifying the registration of operations).	Process Execution and Management	Average	High	High	Import - evidence the import via video, logs, etc., copied in a secure place (encryption), after data transfer to databricks, destroy imported base. Can use PAM	10	Log Transfer via Video	Evidence copy process	Indirect-auto	Manual	On-demand	Satisfactory
										11	Keep a copy in a safe place	Protect data being processed	Indirect-auto	Manual	On-demand	Satisfactory
										12	Destroy lowered base after copy in safe place	Prevent improper copying	Indirect-auto	Manual	On-demand	Satisfactory
										9	Tool to PAM	Monitor Privileged Access	Preventive	Automatic	Daily (multiple times)	Strong
1.1.6	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID and RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Data processing - Absence of documentation supporting records and entries made (Make entries if the document supports justifying the registration of operations).	Process Execution and Management	Average	High	High	Statistics having controls for the activities carried out in the tool.	13	Initial audit to verify that Databricks logs are active	Secure logs	Preventive	Automatic	On-demand	Satisfactory
										14	Check logs with each data load update	confirm that logs are actually working, due to project criticality	Preventive	Automatic	On-demand	Satisfactory
1.1.7	CASEID and RMS Systems Database	Import Database	Import Database of the CASEID eRMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Non-compliance with the contractual terms and/or legal and legal aspects by the professional (Legal non-compliance by the company and/or the employee).	Process Execution and Management	Average	High	High	In the project will be placed all the requirements (SoD, etc). Operator signed a civil accountability.	1	Confidentiality agreement	To make people aware of their limits	Preventive	Manual	On-demand	Satisfactory
										2	Training and Awareness Reinforcement for Project Team	Ensure that everyone knows the project's data confidentiality rules	Preventive	Manual	On-demand	Satisfactory
										5	Segregation of Duties	Do not allow the user to change the segregation of settings	Preventive	Manual	On-demand	Regular
1.1.8	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID eRMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Inadequate training (Lack of knowledge or lack of knowledge/Below how of the requirements of the role).	Process Execution and Management	Average	High	High	Formal course of the foot and validation of the required skills, and for curriculum	15	Formal course of Databricks	Formalize knowledge	Preventive	Manual	On-demand	Regular
1.1.9	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID and RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to carry out behavioral analysis of the industry	Company and/or entity data leakage during import	Process Execution and Management	Average	High	High	Import - evidence the import via video, logs, etc., copied in a secure place (encryption), after data transfer to databricks, destroy imported base. Can use PAM	10	Log Transfer via Video	Evidence copying process	Indirect-auto	Manual	On-demand	Satisfactory
										11	Keep a Copy in a safe place	Protecting data from being stolen	Indirect-auto	Manual	On-demand	Satisfactory
										12	Destroy lowered base after copying to safe place	Prevent improper copying	Indirect-auto	Manual	On-demand	Satisfactory
										9	Tool to PAM	Monitor Privileged Access	Preventive	Automatic	Daily (multiple times)	Strong
1.1.10	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID and RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to carry out behavioral analysis of the industry	Leakage of company and/or entity data - Processing	Process Execution and Management	Average	High	High	Machine to be used must be corporate and in compliance with SB criteria. Implement DLP, Review internet access, mount VLAN if possible prevent USB use, disk encryption and corporate pendrive (if necessary), . Classification of MIP information	16	Log in only from corporate device	Access Origin Control	Preventive	Automatic	Daily (multiple times)	Satisfactory
										17	DLP	Prevent data from being sent to an external environment	Preventive	Automatic	Daily (multiple times)	Strong
										18	VLAN	Segmented environment, separating from the other SBNAI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										19	Crash USB port usage	Prevent data from being sent to an external environment	Preventive	Automatic	Daily (multiple times)	Regular
										20	Disk Cryptographs	Prevent access to the device in the event of loss or theft of the device	Preventive	Automatic	Daily (multiple times)	Satisfactory
										21	Classify information, according to MIP	Define level and who can access the information	Preventive	Manual	Daily (multiple times)	Satisfactory
1.1.11	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID eRMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to carry out behavioral analysis of the industry	Impact on availability and use of data	Process Execution and Management	Low	Low	Low	Disaster scenarios	Accepted Risk	Accepted Risk	Accepted Risk	Accepted Risk	Accepted Risk	Accepted Risk	Accepted Risk
1.1.12	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID and RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to carry out behavioral analysis of the industry	Non-compliance with the LGDP, Subject to fines, administrative and judicial measures. Reputational risks. Exposure to security incidents incident to personal data, such as data loss and exposure.	Privacy and Privacy (LGPD)	High	High	High	previous measures support compliance with the LGDP, RMPD will be notified about the transfer of data Hypothesis Research being validated Receives "left" data The data processing document will be assembled, it will be included in the inventories. RIPD, SI - Data Anonymization, Encryption, Masking, Hashing will be carried out.	22	Contract a third party, and it is the data controller (what he is in charge of the)	Check the Contract or Third processing, and Processing Orders - Suggestions with the AMPD	Preventive	Manual	On-demand	Satisfactory
										23	Definition of a legal hypothesis for data processing	They fit into a research hypothesis	Preventive	Manual	On-demand	Regular
										24	Realization of the RIPD	Assess risks to data subjects that may be caused by the processing	Preventive	Manual	On-demand	Satisfactory
										25	Data Inventory	Recording the processing	Preventive	Manual	On-demand	Satisfactory
										26	Anonymization of data from a certain stage of the process	Hypothesis: Use anonymized data in the stage in which it is ideal to eliminate access to a minimum of stages. Distribution of the data with authorization	Preventive	Manual	On-demand	Satisfactory
										27	Encrypting data in transit and at rest	Ensure data confidentiality	Preventive	Automatic	Daily (multiple times)	Satisfactory
										28	Hashing or CPF e CNPJ	Anonymize data	Preventive	Automatic	Daily (several times)	Strong
1.1.13	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID e RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to carry out behavioral analyses of the industry	Occurrence of fraud, deviations, ethical infractions, illegality, possible risks to customers and stakeholders (depending on the business)	Compliance	Average	High	High	The controls provided for in paragraphs 1.1.1 to 1.1.12 address these risks	1	Confidentiality agreement	To make people aware of their limits	Preventive	Manual	On-demand	Satisfactory
										2	Training and Awareness Reinforcement for the Project Team	Ensure that everyone knows the project's data confidentiality rules	Preventive	Manual	On-demand	Satisfactory
										4	Databricks Security Controls	Evidence of best practices and avoid ctrl misconfiguration	Preventive	Automatic	Daily (multiple times)	Satisfactory
										5	Segregation of Duties	Do not allow the user to change the segregation of settings	Preventive	Manual	On-demand	Regular
										8	Audit	Check level of adherence to policies, standards, etc.	Detective	Manual	Monthly	Satisfactory
										9	Tool to PAM	Monitorare este de acessos privilegiados	Preventive	Automatic	Daily (multiple times)	Strong
										16	Log in only from corporate device	Access Origin Control	Preventive	Automatic	Daily (multiple times)	Satisfactory
										17	DLP	Prevent data from being sent to an external environment	Preventive	Automatic	Daily (multiple times)	Strong
										18	VLAN	Segmented environment, separating from the other SBNI/SBNAI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										19	Crash USB port usage	Prevent data from being sent to an external environment	Preventive	Automatic	Daily (multiple times)	Regular
										21	Classify information, according to MIP	Define level and who can access the information	Preventive	Manual	Daily (multiple times)	Satisfactory
										29	Secure link	Restricted user and access grant, corporate SharePoint style	Preventive	Automatic	On-demand	Satisfactory
										30	Machine isolated from the internet	Prevent improper access or improper sending of data	Preventive	Automatic	Daily (multiple times)	Satisfactory
1.1.14	CASEID and RMS Systems Database	Import Database	Import Database of the CASEID e RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Sanctions from supervisory bodies Payment of fines Lawsuits Damage to image and investments to recover credibility Loss of reliability with stakeholders Loss of customers Loss of market share. Loss of investors Reactive process review	Compliance	Low	High	Medium	The controls provided for in paragraphs 1.1.1 to 1.1.12 address these risks	1	Confidentiality agreement	To make people aware of their limits	Preventive	Manual	On-demand	Satisfactory
										2	Training and Awareness Reinforcement for the Project Team	Ensure that everyone knows the project's data confidentiality rules	Preventive	Manual	On-demand	Satisfactory
										4	Databricks Security Controls	Evidence of best practices and avoid ctrl misconfiguration	Preventive	Automatic	Daily (multiple times)	Satisfactory
										5	Segregation of Duties	Do not allow the user to change the segregation of settings	Preventive	Manual	On-demand	Regular
										8	Audit	Check level of adherence to policies, standards, etc.	Detective	Manual	Monthly	Satisfactory
										9	Tool to PAM	Monitorare este de acessos privilegiados	Preventive	Automatic	Daily (multiple times)	Strong
										16	Log in only from corporate device	Access Origin Control	Preventive	Automatic	Daily (multiple times)	Satisfactory
										17	DLP	Prevent data from being sent to an external environment	Preventive	Automatic	Daily (multiple times)	Strong
										18	VLAN	Segmented environment, separating from the other SBNI/SBNAI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										19	Crash USB port usage	Prevent data from being sent to an external environment	Preventive	Automatic	Daily (multiple times)	Regular
										21	Classify information, according to MIP	Define level and who can access the information	Preventive	Manual	Daily (multiple times)	Satisfactory
1.1.15	CASEID and RMS Systems Database	Import Database	Import Database from CASEID eRMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to carry out behavioral analysis of the industry	Ineffective and inefficient internal controls Non-adherence of the areas to the instituted controls Legal non-compliance	Compliance	Average	High	High	The controls provided for in paragraphs 1.1.1 to 1.1.12 address these risks	8	Audit	Check level of adherence to policies, standards, etc.	Detective	Manual	Monthly	Satisfactory
										14	Check logs with each data load update	Confirm that logs are actually working, due to project criticality	Preventive	Automatic	On-demand	Satisfactory
										21	Classify information, according to MIP	Define level and who can access the information	Preventive	Manual	Daily (multiple times)	Satisfactory
										29	Secure link	Access and restricted user assurance, SharePoint corporate style	Preventive	Automatic	On-demand	Satisfactory
1.1.16	CASEID and RMS Systems Database	Import Database	Import Database of the CASEID e RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Impact - Cyber attack (Incident capable of affecting data, information, assets and services, generating losses resulting from data leakage, arising from a criminal act against networks and/or information systems, with the intention of committing a crime (cyber disorder to obtain financial profit).	Cybernetics	Average	High	High	Check download timeseries.csv links / authenticated user The controls provided for in items 1.1.1 to 1.1.12 address these risks	7	Training and Awareness Reinforcement for the Project Team	Ensure that everyone knows the project's data confidentiality rules	Preventive	Manual	On-demand	Satisfactory
										3	Create Specific Cloud Instance	segregate the data processing environment from the other SBNI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										4	Databricks Security Controls	Evidence of best practices and avoid ctrl misconfiguration	Preventive	Automatic	Daily (multiple times)	Satisfactory
										6	Databricks configuration performed by an expert	Ensure the accuracy of settings	Preventive	Manual	On-demand	Satisfactory
										9	Tool to PAM	Monitorare este de acessos privilegiados	Preventive	Automatic	Daily (multiple times)	Strong
										16	Log in only from corporate device	Access Origin Control Corporate Device	Preventive	Automatic	Daily (several times)	Satisfactory
										18	VLAN	Segmented environment, separating from the other SBNI/SBNAI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										20	Disk Cryptographs	Prevent access to the device in the event of loss or theft of the device	Preventive	Automatic	Daily (multiple times)	Satisfactory
										29	Secure link	Quarantined access and restricted user, SharePoint corporate style	Preventive	Automatic	On-demand	Satisfactory
										30	Internet isolated Machine	Prevent improper access or improper sending of data	Preventive	Automatic	Daily (multiple times)	Satisfactory
										31	Network configuration that has improper traffic	Prevent improper access or improper sending of data	Preventive	Automatic	Daily (multiple times)	Satisfactory
1.1.17	CASEID and RMS Systems Database	Import Database	Import Database of the CASEID e RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Data processing - Cyber attack (Incident capable of affecting data, information, assets and services, generating losses resulting from data leakage, arising from a criminal act against networks and/or information systems, with the intention of committing a crime (cyber disorder to obtain financial profit).	Cybernetics	Average	High	High	Machine isolated from the internet. To access, sites will be defined (IP, network, etc.) The controls provided for in items 1.1.1 to 1.1.12 deal with these risks	2	Training and Awareness Reinforcement for the Project Team	Ensure that everyone knows the project's data confidentiality rules	Preventive	Manual	On-demand	Satisfactory
										3	Create Specific Instance in Cloud	segregate the data processing environment from the other SBNI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										4	Databricks Security Controls	Evidence of best practices and avoid ctrl misconfiguration	Preventive	Automatic	Daily (multiple times)	Satisfactory
										6	Databricks configuration performed by an expert	Ensure the accuracy of settings	Preventive	Manual	On-demand	Satisfactory
										9	Tool to PAM	Monitor Privileged Access	Preventive	Automatic	Daily (multiple times)	Strong
										16	Log in only from corporate device	Access Origin Control	Preventive	Automatic	Daily (multiple times)	Satisfactory
										18	VLAN	Segmented environment, separating from the other SBNI/SBNAI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										20	Disk Cryptographs	Prevent access to the device in the event of loss or theft of the device	Preventive	Automatic	Daily (multiple times)	Satisfactory
										29	Secure link	Access and user restricted grant, SharePoint corporate style	Preventive	Automatic	On-demand	Satisfactory
										30	Internet isolated Machine	Prevent improper access or improper sending of data	Preventive	Automatic	Daily (multiple times)	Satisfactory
										31	Network configuration that has improper traffic	Prevent improper access or improper sending of data	Preventive	Automatic	Daily (multiple times)	Satisfactory
1.1.18	CASEID and RMS Systems Database	Import Database	Import Database of the CASEID e RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Routines or programs that are not processed correctly or completely are not identified, addressed, or handled correctly, impacting data interfaces or transactions performed without user intervention.	Technology	Average	High	High	Appropriate tool - Databricks If trained personnel The controls provided for in items 1.1.1 to 1.1.12 address these risks	7	Training and Awareness Reinforcement for the Project Team	Ensure that everyone knows the project's data confidentiality rules	Preventive	Manual	On-demand	Satisfactory
										4	Databricks Security Controls	Verify evidence	Preventive	Automatic	Daily (multiple times)	Satisfactory
										5	Segregation of Duties	Do not allow the user to change the segregation of settings	Preventive	Manual	On-demand	Regular
										6	Databricks configuration performed by an expert	Ensure the accuracy of settings	Preventive	Manual	On-demand	Satisfactory
										7	Certified Professional Responsible for Configuration	Ensure assertiveness of the Settings	Preventive	Manual	On-demand	Regular
										15	Formal course of Databricks	Formalize knowledge	Preventive	Manual	On-demand	Regular
										21	Classify information, according to MIP	Define level and who can access the information	Preventive	Manual	Daily (multiple times)	Satisfactory
1.1.19	CASEID and RMS Systems Database	Import Database	Import Database of the CASEID eRMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Exposure of unauthorized images/information - due to improper disclosure	Information Security	Average	High	High	The controls provided for in paragraphs 1.1.1 to 1.1.12 address these risks	1	Non-disclosure agreement	To make people aware of their limits	Preventive	Manual	On-demand	Satisfactory
										2	Training and Awareness Reinforcement for the Project Team	Ensure that everyone knows the project's data confidentiality rules	Preventive	Manual	On-demand	Satisfactory
										3	Create Specific Cloud Instance	segregate the data processing environment from the other SBNI/SBNAI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										4	Databricks Security Controls	Verify evidence	Preventive	Automatic	Daily (multiple times)	Satisfactory
										5	Segregation of Duties	Do not allow the user to change the segregation of settings	Preventive	Manual	On-demand	Regular
										8	Audit	Check level of adherence to policies, standards, etc.	Detective	Manual	Monthly	Satisfactory
										9	Tool to PAM	Monitor Privileged Access	Preventive	Automatic	Daily (multiple times)	Strong
										16	Log in only from corporate device	Access Origin Control	Preventive	Automatic	Daily (multiple times)	Satisfactory
										17	DLP	Prevent data from being sent to an external environment	Preventive	Automatic	Daily (multiple times)	Strong
										18	VLAN	Segmented environment, separating from the other SBNI/SBNAI environments	Preventive	Automatic	Daily (multiple times)	Satisfactory
										19	Crash USB port usage	Prevent data from being sent to an external environment	Preventive	Automatic	Daily (multiple times)	Regular
										21	Classify information, according to MIP	Define level and who can access the information	Preventive	Manual	Daily (multiple times)	Satisfactory
										27	Encrypt data in transit and at rest	Ensure data confidentiality	Preventive	Automatic	Daily (multiple times)	Satisfactory
										29	Secure link	Access and restricted user assurance, Sharepoint corporate style	Preventive	Automatic	On-demand	Satisfactory
										30	Internet isolated Machine	Prevent improper access or improper sending of data	Preventive	Automatic	Daily (multiple times)	Satisfactory
										31	Network configuration that has improper traffic	Prevent improper access or improper sending of data	Preventive	Automatic	Daily (multiple times)	Satisfactory
1.1.20	CASEID and RMS Systems Database	Import Database	Import Database of the CASEID e RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Import - Access Control Failed - Unauthorized User Access	Information Security	Average	High	High	MP shall take the necessary actions to make the data available in a secure manner and by secure means. Check for the possibility of data being sent from cloud to cloud. (No check possibility) Implemented SoD The controls provided for in items 1.1.1 to 1.1.12 address these risks	5	Segregation of Duties	Do not allow the user to change the segregation of settings	Preventive	Manual	On-demand	Regular
										8	Audit	Check level of adherence to policies, standards, etc.	Detective	Manual	Monthly	Satisfactory
										9	Tool to PAM	Monitor Privileged Access	Preventive	Automatic	Daily (multiple times)	Strong
1.1.21	CASEID and RMS Systems Database	Import Database	Import Database from the CASEID e RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Data Processing - Failure in access control - Unauthorized user access	Information Security	Average	High	High	SoD implemented other controls	5	Segregation of Duties	Do not allow the user to change the segregation of settings	Preventive	Manual	On-demand	Regular
										8	Audit	Check level of adherence to policies, standards, etc.	Detective	Manual	Monthly	Satisfactory
										9	Tool to PAM	Monitor Privileged Access	Preventive	Automatic	Daily (multiple times)	Strong
1.1.22	CASEID and RMS Systems Database	Import Database	Import Database of the CASEID e RMS systems to transfer this data between SBNAI SP and the Ministry of Labor, to be carried out behavioral analysis of the industry	Releasing Access to Unauthorized Persons (Releasing Access to Unauthorized Persons).	Information Security	High	High	High	Access uses MFA and SoD, managed by a competent area and other controls	32	Multi-Factor Authentication	Ensure confidentiality by increasing identity verification	Preventive	Automatic	Daily (multiple times)	Strong
										5	Segregation of Duties	Do not allow the user to change the segregation of settings	Preventive	Manual	On-demand	Regular
										8	Audit	Check level of adherence to policies, standards, etc.	Detective	Manual	Monthly	Satisfactory
										9	Tool to PAM	Monitor Privileged Access	Preventive	Automatic	Daily (multiple times)	Strong