



GRUPO DE EMPRESAS CHILQUINTA
GERENCIA TECNOLOGIA

Identificación:
CS GT SGTI PO 17

Fecha Creación:
01/01/2011

Fecha Modificación:
10-12-2024

Versión:
0

PROCEDIMIENTO OPERATIVO

RESPALDO DE LA INFORMACIÓN
INFORMATION BACKUP

Revisado por:
Alfredo Martínez
Fecha: 10-12-2024

Aprobado por:
Wei Zhonghua
Fecha: 10-12-2024

1. OBJETIVO

El objetivo del siguiente documento es definir un procedimiento para la administración y generación de los respaldos de información del grupo de empresas Chilquinta.

2. ALCANCE

Procedimiento bajo alcance de Chilquinta Servicios S.A. aplicable bajo responsabilidad del área de Sistemas e Infraestructura, para todos los servicios productivos ubicados en servidores a responsabilidad del área y ubicados en ambos centros de datos pertenecientes al Grupo de Empresas Chilquinta.

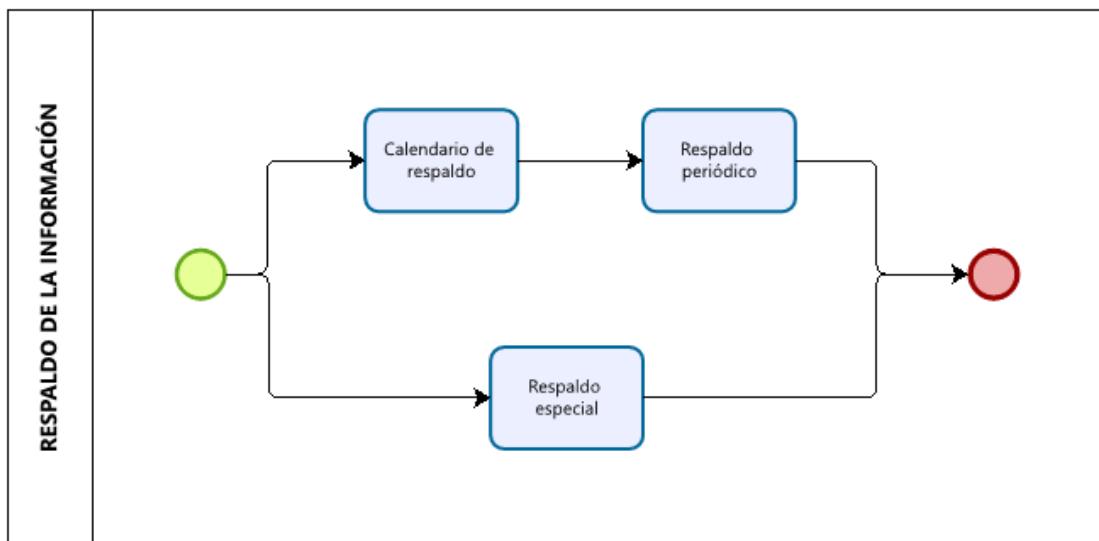
3. RESPONSABILIDAD Y AUTORIDAD

- Jefe de Sistemas e Infraestructura.
- Ingenieros de Sistemas
- Administrador de plataforma y Arquitecto de Infraestructura TI
- Administradores de Base de Datos
- Grupo de Operaciones

4. DEFINICIONES Y ABREVIACIONES

DRP: Plan de recuperación ante desastres.

5. DIAGRAMA DE FLUJO



6. CONTENIDO

6.1. Entradas y salidas del proceso

- Se define como entrada del proceso la información a ser respaldada.
- Se define como salida del proceso los informes diarios y la bitácora de respaldos.

6.2. Respaldo por seguridad de datos

6.2.1. Propósito

Este procedimiento norma el proceso de Respaldo de la información necesaria para una correcta continuidad operacional de Tecnologías de la información, la plataforma a ser respaldada tiene directa relación con los servicios que son parte del DRP y otros servicios que sean requeridos como los repositorios de información y servidores de aplicación.

6.2.2. Definiciones

Es responsabilidad de Sistemas e Infraestructura, el resguardo de la información contenida en las bases de datos, repositorios de información y servidores de aplicación.

Es responsabilidad del Ingeniero de Sistemas velar por el correcto funcionamiento de la plataforma de respaldo.

El administrador de plataforma será el responsable de ejecutar las tareas que estén relacionadas con la administración de la plataforma de respaldo y escalamientos ante incidentes con el proveedor que brinda el soporte.

Es responsabilidad del Ingeniero de Sistemas en conjunto con el Arquitecto de Infraestructura TI y cuando corresponda con los administradores de Bases de Datos, construir el calendario de respaldo.

El procedimiento actual considera la ejecución de respaldos con la siguiente modalidad y periodicidad:

#	Respaldo	Modalidad	Periodicidad
1	SQL Server	Full	Fin de Semana
2	SQL Server	Incremental	Diario
3	BD PowerON	Full	Diario
4	BD Open Smartflex	Full	Fin de Semana
5	BD Open Smartflex	Incremental	Diario
6	FS Open Smartflex	Full	Fin de Semana
7	FS Open Smartflex	Incremental	Diario
8	SAP	Full	Diario
9	DMZ	Full	Fin de Semana
10	DMZ	Incremental	Diario
11	DTE	Full	Fin de Semana
12	DTE	Incremental	Diario
13	Aplicativos PO y EO	Full	Fin de Semana

14	Servidores ME	Full	Fin de Semana
15	Servidores SMAX (On-premise)	Full	Fin de Semana
16	Servidores Proficy	Full	Fin de Semana
17	Servidores SCADA/DMS	Full	2 sábados al mes
18	Servidores SCADA/DMS	Incremental	Diario
19	Servidores FEP SCADA	Incremental	Diario
20	BD Históricas SCADA	Full	Semanal
21	BD Históricas SCADA	Incremental	Diario
22	Servidor APM	Full	Fin de Semana

Cada vez que se ponga en producción un nuevo sistema o se agregue una nueva base de datos, es responsabilidad del Jefe de Proyectos o Jefe de Desarrollo de Sistemas y Proyectos Tecnológicos notificar al área de Infraestructura los respaldos requeridos.

Es responsabilidad del Operador de Turno 1, revisar el término normal de todos los procesos de respaldos, sean estos automáticos o los pedidos expresamente. En este último caso, se deberá además informar al solicitante del éxito o fracaso de su solicitud.

Además, es responsabilidad del Operador de Turno 1, retirar las cintas diarias de respaldo y trasladarlas a la bóveda de seguridad, reemplazando éstas por nuevas cintas de forma, de asegurar físicamente las cintas en caso de alguna catástrofe.

Es responsabilidad del Operador Turno 2, revisar la unidad de respaldo en cuanto a la disponibilidad de cintas para el respaldo nocturno, de manera que no exista ninguna dificultad con el proceso. En caso de no existir el espacio disponible necesario, deberá incorporar una nueva cinta en el pool de respaldo correspondiente, procediendo a trasladar la cinta llena a la bóveda de respaldo.

6.2.3. Supervisión y Control

El Ingeniero de Sistemas tiene el deber de velar por el adecuado funcionamiento de esta plataforma y deberá instruir a los Operadores para que estén adecuadamente preparados y actualizados en el desarrollo de ésta delicada labor.

Es responsabilidad del Ingeniero de Sistemas realizar la supervisión necesaria y las inspecciones correspondientes con el fin de velar por el adecuado cumplimiento de esta norma.

Es responsabilidad del Administrador de Bases de datos, informar cualquier problema detectado en los respaldos a nivel de Base de Datos.

6.2.4. Respaldo por seguridad de Sistemas de información

6.2.4.1. Propósito

Este procedimiento norma como y quien deberá solicitar el respaldo periódico de la información propia de un Sistema de Información que requiera respaldos especiales, y quien estaría autorizado para solicitar la restauración de dicho respaldo.

6.2.4.2. Definiciones

Se debe partir de la premisa que toda la información contenida en las bases de datos corporativas está resguardada por los procedimientos de seguridad, por tanto, no se requieren procedimientos de respaldo adicionales, con la excepción de lo siguiente:

1. Cuando se necesite mantener la historia de la información, por periodos superiores a lo que cubre el respaldo de seguridad.
2. Cuando se requiera disponer de una imagen puntual de la información a causa de un cambio importante, esta historia debe tener una duración específica.
3. Cuando se necesite contar con historia de la información propia de los procesos, información que posteriormente no quede, en contenido o en formato, disponible en las bases de datos,

Será el Jefe de Proyectos, quien deberá definir el tipo de respaldos, la periodicidad y el periodo de retención de éstos.

Será el Ingeniero de Sistemas quien deberá incorporar este tipo de respaldos a los procedimientos de respaldo.

Es responsabilidad de Operaciones, velar por que se estén manteniendo adecuadamente resguardadas y rotuladas las cintas de este tipo de respaldos, velando a su vez porque exista una copia en bóveda interna y otra en bóveda externa.

Es responsabilidad del Operador de Turno 1, revisar el término normal de todos los procesos de respaldos, especialmente de este tipo de respaldo, los que, en caso de no ser exitosos, deberán tener un procedimiento alternativo para salvar la información, antes que esta sea modificada por el sistema de información.

Sólo el jefe de Sistemas e Infraestructura tiene la autorización para solicitar la restauración de dicha información, en caso de ausencia de éste, la responsabilidad recae en su reemplazante o en el Subgerente de Telecomunicaciones y Tecnologías de la Información.

Para solicitar la restauración de parte de la información respaldada, el Jefe de Desarrollo de Sistemas y Proyectos tecnológicos deberá solicitar formalmente al Jefe de Sistemas e Infraestructura que se procesa a restaurar dicha información, indicando la o las fechas que se restaurarán y los motivos por el cual se restauran, esta solicitud deberá ir con copia al Subgerente de Telecomunicaciones y Tecnologías de la Información, además del administrador usuario si existiese.

Es obligatorio pasar por un control de cambios para todo tipo de modificación en la programación y/o pausado de cualquier tipo de respaldo, considerando el "Procedimiento Control de Cambios al Ambiente

Operativo”, esto también se debe realizar para las copias de mandante en SAP y clonaciones en PowerON y OSF.

6.2.4.3. Supervisión y Control

El Ingeniero de Sistemas, tiene el deber de velar por el adecuado funcionamiento de esta plataforma y deberá instruir a los Operadores para que estén adecuadamente preparados y actualizados en el desarrollo de ésta delicada labor.

Es responsabilidad del Ingeniero de Sistemas realizar la supervisión necesaria y las inspecciones correspondientes con el fin de velar por el adecuado cumplimiento de esta norma.

Es responsabilidad del Administrador de Bases de datos, informar cualquier problema detectado en los respaldos a nivel de Base de Datos.

6.2.5. Mantención de Respaldos y Bitácoras.

6.2.5.1. Propósito

Este procedimiento norma las responsabilidades en cuanto al registro necesario en las bitácoras de respaldo, como a su vez a la mantención de cintas en la bóveda interna de la empresa.

6.2.5.2. Definiciones

En las bitácoras de respaldos se deberá contar con la siguiente información:

1. Grupo de respaldo al que corresponde
2. Fecha del respaldo.
3. Inicio
4. Término
5. Descripción
6. Estado
7. Pool de respaldo
8. Observación

Es responsabilidad de Operaciones, velar por que se estén manteniendo adecuadamente completas y actualizadas las respectivas bitácoras.

Una vez al mes se deberá verificar cualquiera de las bitácoras con la existencia en las bóvedas respectivas, y en caso de existir anomalías, proceder a su regularización inmediata.

Es responsabilidad del Operador de Turno completar adecuadamente cada una de las bitácoras, sean estas de respaldos o de traslado de cintas desde y hacia las respectivas bóvedas.

En caso de requerirse alguna cinta, es el Operador de turno quien deberá acceder a la bóveda respectiva y colocar la cinta en la unidad de respaldo.

Es obligatorio pasar por un control de cambios para todo tipo de modificación en la programación y/o pausado de cualquier tipo de respaldo, considerando el “Procedimiento Control de Cambios al Ambiente Operativo”, esto también se debe realizar para las copias de mandante en SAP y clonaciones en PowerON y OSF.

6.2.5.3. Supervisión y Control

El jefe de Sistemas e Infraestructura deberá velar periódicamente por las bitácoras, verificar que la información contenida en éstas sea fidedigna y que se encuentren absolutamente actualizadas.

El responsable de Operaciones debe realizar las inspecciones correspondientes con el fin de velar por el adecuado cumplimiento de esta norma.

7. NORMATIVA VIGENTE

No Aplica.

8. REFERENCIAS

Procedimiento Control de Cambios.

Procedimiento Rotación y Traslado de Cintas.

9. ASUNTOS ÉTICOS

Consultas o inquietudes relacionadas con temas éticos pueden ser realizadas al encargado de cumplimiento (Gerente Legal) al fono: 322452289.

10. HISTORIAL DE CAMBIOS

Nº Versión	Fecha Vigencia	Comentario	Elaborado por	Revisado por	Aprobado por
1	30/06/20211	Creación y revisión de procedimiento.	NA	NA	NA
2	11/01/2017	Revisión de procedimiento.	NA	NA	NA
3	30/05/2018	Revisión de procedimiento.	NA	NA	NA
4	02/09/2019	Modificación de cargos y áreas.	NA	NA	NA
5	02/07/2020	Revisión de procedimiento.	NA	NA	NA
6	20/07/2020	Se incorpora información de servicios SCADA y NO SCADA.	NA	NA	NA

7	11/11/2021	Revisión de procedimiento, actualización de empresa, actualización de logo y actualización de información incluida en procedimiento.	NA	NA	NA
8	31/01/2022	Revisión y actualización de procedimiento según cambios GED.	NA	NA	NA
9	21/09/2022	Incorporación de servicios de respaldo en cinta para BD históricas SCADA.	NA	NA	NA
10	09/01/2023	Incorporación de obligatoriedad en modificación de programaciones y/o cambios, junto con la inclusión de información respecto a la periodicidad y servicios de respaldo.	NFG	NA	NA
0	10-12-2024	Actualización de formato, según Procedimiento Control y Gestión de Documentos Corporativos	Jesus Ayala	Alfredo Martínez	Wei Zhonghua

11. ANEXOS Y REGISTROS

Registros: Los registros digitales se almacenarán según se indique en la planilla de gestión de configuración del área de Sistemas e Infraestructura.



**CHILQUINTA GROUP OF COMPANIES
TECHNOLOGY MANAGEMENT**

Identification:
CS GT SGTI PO 17

Creation date:
01/01/2011

Modification date:
10-12-2024

Version:
0

OPERATING PROCEDURE

**INFORMATION BACKUP
RESPALDO DE LA INFORMACIÓN**

Reviewed by:
Alfredo Martínez
Date: 10-12-2024

Approved by:
Wei Zhonghua
Date: 10-12-2024

1. OBJECTIVE

The objective of the following document is to define a procedure for the administration and generation of the information backups of the Chilquinta group of companies.

2. SCOPE

Procedure under the scope of Chilquinta Servicios S.A. applicable under the responsibility of the Systems and Infrastructure area, for all productive services located on servers under the responsibility of the area and located in both data centers belonging to the Chilquinta Group of Companies.

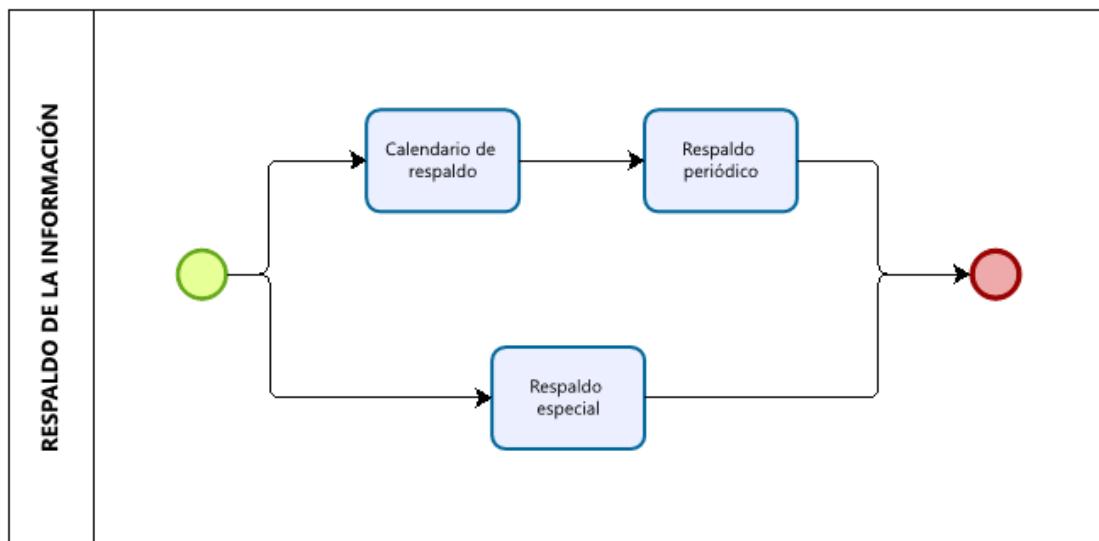
3. RESPONSIBILITY AND AUTHORITY

- Head of Systems and Infrastructure.
- Systems Engineers
- Platform Manager and IT Infrastructure Architect
- Database Administrators
- Operations Group

4. DEFINITIONS AND ABBREVIATIONS

DRP: Disaster Recovery Plan

5. FLOWCHART



6. CONTENT

6.1 Process inputs and outputs

- The information to be backed up is defined as input to the process.
- The output of the process is defined as the daily reports and the backup log.

6.1.1 Data security backup

6.1.1.1 Purpose

This procedure regulates the process of Backup of the information necessary for a correct operational continuity of Information Technologies, the platform to be supported has direct relationship with the services that are part of the DRP and other services that are required such as information repositories and application servers.

6.1.1.2 Definitions

It is the responsibility of Systems and Infrastructure, the protection of the information contained in the databases, information repositories and application servers.

It is the responsibility of the Systems Engineer to ensure the proper functioning of the backup platform.

The platform administrator will be responsible for executing the tasks that are related to the administration of the backup platform and escalations in case of incidents with the provider that provides the support.

It is the responsibility of the System Engineer in conjunction with the IT Infrastructure Architect and where appropriate with the Database Administrators, to build the backup schedule.

The current procedure considers the execution of endorsements with the following modality and periodicity:

#	Backup	Modality	Periodicity
1	SQL Server	Full	Weekend
2	SQL Server	Incremental	Daily
3	BD PowerON	Full	Daily
4	BD Open Smartflex	Full	Weekend
5	BD Open Smartflex	Incremental	Daily
6	FS Open Smartflex	Full	Weekend
7	FS Open Smartflex	Incremental	Daily
8	SAP	Full	Daily
9	DMZ	Full	Weekend
10	DMZ	Incremental	Daily
11	DTE	Full	Weekend
12	DTE	Incremental	Daily
13	PO and EO applications	Full	Weekend

#	Backup	Modality	Periodicity
14	ME Servers	Full	Weekend
15	SMAX (On-premise) servers	Full	Weekend
16	Proficy Servers	Full	Weekend
17	SCADA/DMS Servers	Full	2 Saturdays per month
18	SCADA/DMS Servers	Incremental	Daily
19	FEP SCADA Servers	Incremental	Daily
20	SCADA Historical DB	Full	Weekly
21	SCADA Historical DB	Incremental	Daily
22	APM Server	Full	Weekend

Each time a new system is put into production or a new database is added, it is the responsibility of the Project Manager or Head of Systems Development and Technological Projects to notify the Infrastructure area of the required endorsements.

It is the responsibility of the Shift Operator 1 to review the normal term of all backup processes, be they automatic or expressly ordered. In the latter case, the applicant must also be informed of the success or failure of his application.

In addition, it is the responsibility of Shift Operator 1 to remove the daily backup tapes and move them to the security vault, replacing these with new shape tapes, to physically secure the tapes in case of a catastrophe.

It is the responsibility of Operator Shift 2 to review the backup unit for the availability of tapes for the night backup, so that there is no difficulty with the process. If there is no available space, you must incorporate a new tape in the corresponding backup pool, proceeding to move the full tape to the backup vault.

6.1.1.3 Supervision and Control

The Systems Engineer has the duty to ensure the proper functioning of this platform and must instruct the Operators to be adequately prepared and updated in the development of this delicate work.

It is the responsibility of the Systems Engineer to perform the necessary supervision and the corresponding inspections in order to ensure proper compliance with this standard.

It is the responsibility of the Database Administrator to report any problems detected in the backups at the Database level.

6.2 Information Systems Security Backup

6.2.1 Purpose

This procedure is as a rule and who should request the periodic backup of the information of an Information System that requires special backups, and who would be authorized to request the restoration of such backup.

6.2.2 Definitions

It should be assumed that all information contained in corporate databases is protected by security procedures, therefore, no additional backup procedures are required, with the exception of the following:

1. When information history needs to be maintained, for periods longer than what the security backup covers.
2. Where a timely picture of the information is required due to a major change, this story should be of a specific duration.
3. When it is necessary to have a history of the information of the processes, information that subsequently does not remain, in content or format, available in the databases,

It will be the Project Manager, who will define the type of backups, the periodicity and the retention period of these.

It will be the Systems Engineer who will have to incorporate this type of backup to the backup procedures.

It is the responsibility of Operations to ensure that the tapes of this type of backing are kept properly protected and labeled, ensuring that there is a copy in an internal vault and another in an external vault.

It is the responsibility of the Shift Operator 1 to review the normal term of all backup processes, especially this type of backup, which, if not successful, must have an alternative procedure to save the information, before it is modified by the information system.

Only the Head of Systems and Infrastructure has the authorization to request the restoration of such information, in the absence of this, the responsibility lies with his replacement or with the Assistant Manager of Telecommunications and Information Technologies.

To request the restoration of some of the information supported, the Head of Systems Development and Technological Projects must formally request the Head of Systems and Infrastructure that is processed to restore such information, indicating the date or dates that will be restored and the reasons for which they are restored, this request must go with a copy to the Deputy Manager of Telecommunications and Information Technologies, in addition to the user administrator if it exists.

It is mandatory to go through a change control for any type of modification in the programming and/or paused of any type of backup, considering the "Change Control Procedure to the Operational Environment", this must also be done for the copies of constituents in SAP and clones in PowerON and OSF.

6.2.3 Supervision and Control

The Systems Engineer has the duty to ensure the proper functioning of this platform and must instruct the Operators to be adequately prepared and updated in the development of this delicate work.

It is the responsibility of the Systems Engineer to perform the necessary supervision and the corresponding inspections in order to ensure proper compliance with this standard.

It is the responsibility of the Database Administrator to report any problems detected in the backups at the Database level.

6.3 Maintenance of Backups and Logs

6.3.1 Purpose

This procedure regulates the responsibilities regarding the necessary registration in the backup logs, as well as the maintenance of tapes in the internal vault of the company.

6.3.2 Definitions

The following information should be included in the backup logs:

1. Support group to which it belongs
2. Date of endorsement.
3. Start
4. Term
5. Description
6. Status
7. Backup Pool
8. Observation

It is the responsibility of Operations to ensure that the respective logs are kept properly complete and up to date.

Once a month, any of the logs must be verified with the existence in the respective vaults, and in case of anomalies, proceed to their immediate regularization.

It is the responsibility of the Shift Operator to properly complete each of the logs, whether these are backups or moving tapes to and from the respective vaults.

In the event that any tape is required, it is the Operator of the day who must access the respective vault and place the tape in the backup unit.

It is mandatory to go through a change control for any type of modification in the programming and/or paused of any type of backup, considering the “Change Control Procedure to the Operational Environment”, this must also be done for the copies of constituents in SAP and clones in PowerON and OSF

6.3.3 Supervision and Control

The Head of Systems and Infrastructure shall regularly monitor the logs, verify that the information contained therein is reliable and that they are absolutely up-to-date.

The Operations Officer should carry out the appropriate inspections to ensure proper compliance with this standard.

7. REGULATIONS IN FORCE

Does not apply.

8. REFERENCES

Change Control Procedure.

Tape Rotation and Transfer Procedure.

9. ETHICAL ISSUES

Inquiries or concerns related to ethical issues can be made to the compliance officer (Legal Manager) at the phone number: 322452289.

10. CHANGE HISTORY

Version No	Effective Date	Comment	Prepared by	Reviewed by	Approved by
1	6/30/20211	Creation and revision of procedure.	NA	NA	NA
2	01/11/2017	Procedural review.	NA	NA	NA
3	30/05/2018	Procedural review.	NA	NA	NA
4	02/09/2019	Modification of charges and areas.	NA	NA	NA
5	02/07/2020	Procedural review.	NA	NA	NA
6	20/07/2020	SCADA and NON-SCADA service information is incorporated.	NA	NA	NA
7	11/11/2021	Procedure review, company update, logo update and update of information included in procedure.	NA	NA	NA
8	01/31/2022	Review and update of procedure according to GED changes.	NA	NA	NA
9	09/21/2022	Incorporation of tape backup services for SCADA historical databases.	NA	NA	NA
10	09/01/2023	Incorporation of mandatory changes in schedules and/or changes, along with the inclusion of information on periodicity and back-up services.	NFG	NA	NA
0	10-12-2024	Format update, according to Procedure Control and Management of Corporate Documents	Jesus Ayala	Alfredo Martínez	Wei Zhonghua

11. ANNEXES AND RECORDS

Records: The digital records will be stored as indicated in the configuration management form of the Systems and Infrastructure area.