SIGEN
Sindicatura General de la Nación
Presidencia de la Nación

INFORME de AUDITORÍA

CONICET

Ministerio de Ciencia, Tecnología e Innovación – Consejo Nacional de Investigaciones Científicas y Técnicas

Controles de la Gestión de la Tecnología Información, especialmente de las acciones de resguardo implementadas.

Noviembre 2023

CONICET

MINISTERIO DE CIENCIA, TECNOLOGÍA E INNOVACIÓN – CONSEJO NACIONAL DE INVESTIGACIONES CIENTÍFICAS Y TÉCNICAS

Controles de la Gestión de la Tecnología de Información, y especialmente de las acciones de resguardo implementadas

TABLA DE CONTENIDO

SIGLARIO

CPD: Centro de Procesamiento de Datos.
OTRS: (Open-source Ticket Request System) “Ticketera Sistema de Mesa de Ayuda Configurable”.
SLA: (Service Level Agreement) “Acuerdo de Nivel de Servicio”.
PCI (Plan de Contingencia Informático)

INFORME EJECUTIVO

SIGEN Sindicatura General de la Nación Presidencia de la Nación

Noviembre de 2023

CONICET - *Consejo Nacional de Investigaciones Científicas y Técnicas.* Ministerio de Ciencia, Tecnología e Innovación.

Controles de la Gestión de la Tecnología de Información, y especialmente de las acciones de resguardo implementadas.

POR QUÉ SE REALIZÓ ESTE INFORME. OBJETIVO Y ALCANCE

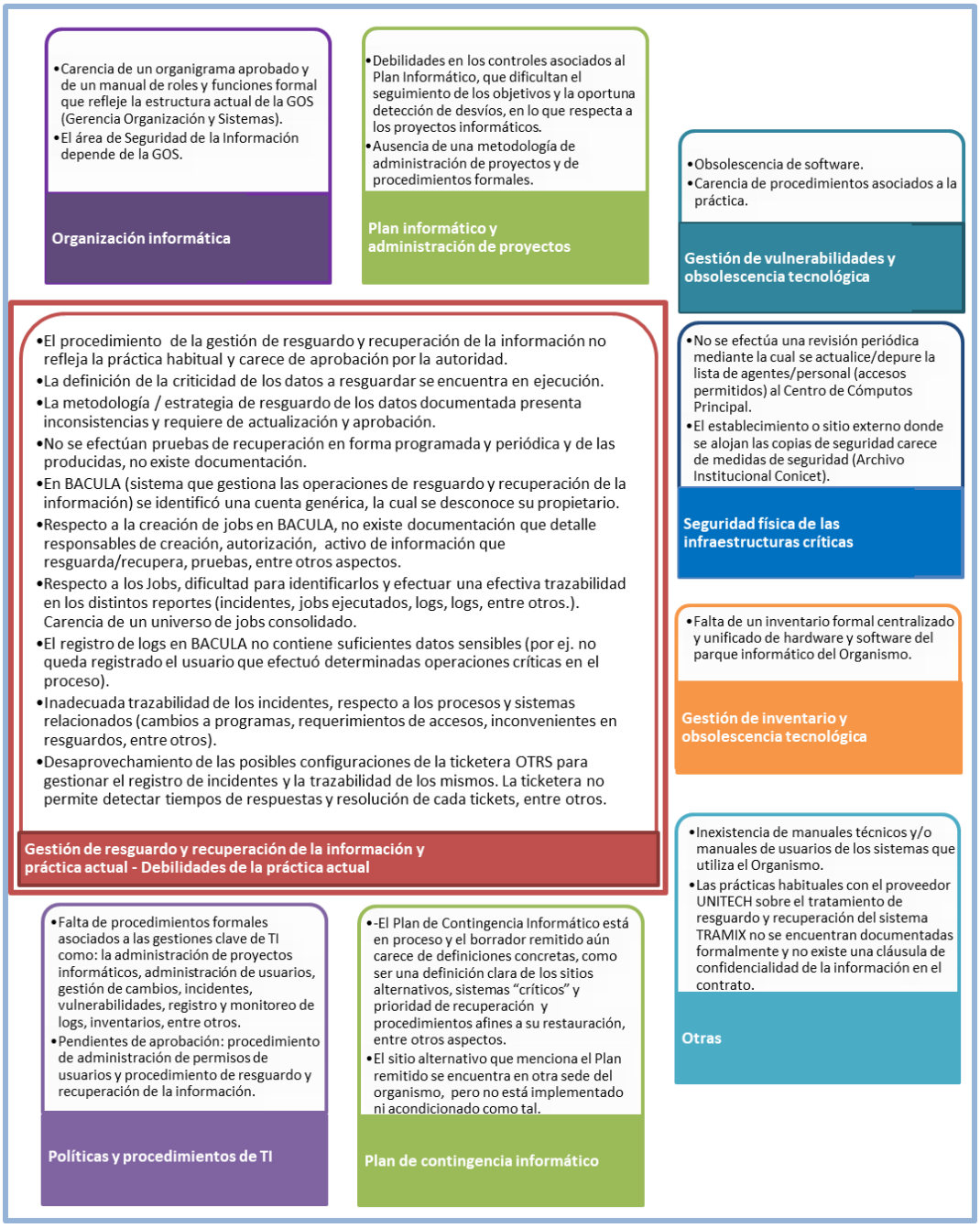
La presente auditoría se encaró por la relevancia del CONICET y fue iniciada según nota NO-2023-31045394-APN-SO#SIGEN.

El objetivo fue analizar los controles relacionados con la gestión de las actividades informáticas desarrolladas en el CONICET, y en lo que respecta particularmente a la gestión de resguardo y recuperación de la información implementada.

El trabajo fue realizado entre abril y agosto 2023, y la opinión del auditado fue recibida en octubre de 2023.

RESULTADOS DE LA AUDITORÍA

Se expone una síntesis de las principales observaciones surgidas de esta labor.



QUÉ ACCIONES SE ENCARARON COMO CONSECUENCIA DEL INFORME DE SIGEN	PRINCIPALES RECOMENDACIONES SIGEN
Respecto a las observaciones identificadas, el CONICET ha encarado acciones y formulado cursos de acción alineados a las recomendaciones efectuadas por SIGEN para diversos señalamientos, estableciendo responsables y plazos para las medidas a instrumentar.	A continuación, se detallan las principales recomendaciones para la regularización de los puntos señalados en el Informe: ➧ Desarrollar e implementar los procedimientos clave de TI faltantes (gestión de usuarios, registro, revisión y monitoreo de logs, licencias de software, seguridad física, gestión de cambios a programas/jobs/scripts, registro y monitoreo de incidentes, vulnerabilidades, entre otros) y actualizar los procedimientos existentes (gestión de usuarios, resguardo y recuperación de la información, entre otros). Documentar la evidencia de su aprobación e indicar sus fechas de vigencia. ➧ Contemplar en el procedimiento de resguardo y recuperación en elaboración, todos los aspectos y controles asociados a esta práctica, asegurando que el mismo refleje la operatoria actual del proceso. Aprobar el procedimiento por la autoridad. Documentar formalmente el criterio para clasificar los activos y/o utilizar una metodología aprobada, a modo de establecer la criticidad de los mismos y establecer prioridades al momento de definir su resguardo y recuperación. Consolidar los Jobs programados para resguardo y recuperación, y mantener el universo actualizado de los jobs ante cada modificación. Considerar configurar en la herramienta BACULA, que los logs registren datos sensibles, como ser los usuarios que efectúan tareas en el proceso, a modo de permitir efectuar trazabilidad. ➧ Desarrollar un plan de contingencia informática formal que cubra integralmente los eventuales siniestros que pudieran afectar la continuidad de los servicios de procesamiento de información del CONICET y el cómo proceder ante esto. ➧ Propiciar que las versiones del software cuenten con el soporte del proveedor correspondiente, a fin de obtener el rendimiento correcto en los servidores donde residen las aplicaciones críticas del Organismo. ➧ Mejorar las condiciones de seguridad del establecimiento en el cual, actualmente, se resguardan las copias de seguridad. ➧ Obtener la aprobación formal de la estructura actual de la GOS y consolidar en un solo documento las misiones y funciones de cada sector que la compone. Asignar las responsabilidades por la Seguridad de la Información a un área independiente de la unidad de TI, a modo de constituir de ese modo, un mecanismo de control por oposición. ➧ Incorporar al plan, según corresponda al plan estratégico o plan operativo, los aspectos que reflejen los proyectos y tareas relacionados con la tecnología informática. Contar con una metodología para la administración de proyectos que respalde todas las acciones a realizar para el control y seguimiento de cumplimiento de proyectos. ➧ Se sugiere analizar la conveniencia de contar con una mesa de ayuda o similar que centralice todos los incidentes/tickets. Adoptar o bien adaptar la herramienta que apoya la gestión de incidentes y cambios para asegurar una efectiva trazabilidad. ➧ Formalizar un inventario formal de hardware y software que reúna los detalles técnicos antes mencionados y se concentre la información, de ser posible, en una única herramienta. ➧ Documentar, actualizar y consolidar toda la documentación técnica y funcional de los sistemas, especificando los módulos con su descripción y funcionalidad y las interfaces que tienen vinculación. A partir del informe preliminar recibido, el CONICET ha encarado un plan de acción alineado a lo recomendado por SIGEN. La consideración de las recomendaciones efectuadas por SIGEN, permitirá reducir los riesgos que surgen de los aspectos observados, por lo que se sugiere efectuar el seguimiento de los avances en el tema.

INFORME ANALÍTICO

1 OBJETIVO

Auditar los controles de la gestión de la tecnología de la información, especialmente en el grado de implementación y características de la gestión de resguardo y recuperación de la información implementadas en el Consejo Nacional de Investigaciones Científicas y Técnicas (en adelante, CONICET).

2 ALCANCE

El trabajo realizado abarcó el relevamiento y evaluación de los procedimientos de control relacionados con la gestión de las actividades informáticas desarrolladas en el CONICET, y en lo que respecta particularmente a la gestión de resguardo y recuperación de la información implementada.

Las tareas se basaron en lo informado en la nota de fecha 21 de marzo de 2023, NO-2023-31045394-APN-SO#SIGEN, a través de la cual SIGEN comunica al CONICET el inicio del proyecto de auditoría.

La revisión se llevó a cabo mediante el análisis de documentación recibida y relevamientos entre los meses de abril de 2023 a agosto 2023, habiéndose recibido la opinión del auditado el 26 de octubre 2023, mediante la NO-2023-127399355-APN-GOYS#CONICET.

3 TAREA REALIZADA

Las tareas consistieron en:

1. Entrevistas mantenidas con personal de las siguientes áreas del CONICET:

   - Gerencia de Organización y Sistemas,
   - Dirección de Gestión de Usuarios y Red,
   - Dirección de Ingeniería de Procesos,
   - Área de la Seguridad de la Información,
   - Área de Operaciones.

2. Revisión de los controles relativos a la gestión de la tecnología informática.

3. Relevamiento de la gestión de resguardo y recuperación de la información y análisis de documentación obtenida.

4. Ejecución de prueba sobre los procesos de resguardo y recuperación producidos en junio 2023, considerando los siguientes reportes provistos por el auditado:

Prueba de Resguardo mensual y traslado a sitio externo	
Se solicitó:	***Se recibió:***
"Prueba: Captura de los backup realizados en un periodo con su estado (fallido, exitoso, interrumpido), con el detalle de su cinta y rotulado del medio. (Debería ser la última externalización.)"	***Jobs + Externalizaciones.xlsx:*** *archivo que contiene las tareas de resguardo (Jobs) ejecutadas en el mes de junio del corriente.*
	Solapa 1: Junio TODO Cinta y Disco
	Solapa 2: Junio SOLO Externalizado *(Detalle de todas las cintas que se mandaron al archivo)*
	Solapa 3: Cintas Externalizadas TODAS *(Detalle de los Jobs que se incluyeron)*
Prueba de Trazabilidad de Logs en Bacula	
Se solicitó:	***Se recibió:***
"Remitir los logs, si es extenso, del mes de junio"	***BACULA.log.2.gz:*** registro de logs de las tareas de resguardo (Jobs) ejecutadas en el mes de junio del corriente.
Análisis Jobs en Bacula	
Se solicitó:	***Se recibió:***
"Listado de jobs programados de este año, explicar cómo se programa (schedulea, cómo sabe qué cinta asignar, etc.) y si se documenta, como se pone en producción."	***JobsEnabled20230811.xlsx:*** listado de las tareas de resguardo (universo de Jobs).
Análisis Inventario de Hardware y Software:	
Se solicitó:	***Se recibió:***
"Inventarios de Hardware y Software (indicar versiones).	***SERVIDORES - Hostnames.xlsx:*** inventario de activos de información, en proceso, (Jobs, servidores y servicios de los Jobs, entre otros).
Prueba trazabilidad incidentes de resguardo/recuperación	
Se solicitó:	***Se recibió:***
"Por favor enviar un reporte de la herramienta con los incidentes cargados a la fecha, al menos que abarque un año. Incluir datos de tiempo de respuesta, y resolución, de existir."	***Reporte_Backup.xslx*** (universo de incidentes desde marzo a junio). *"Se adjunta una* ***impresión de 1 ticket completo*** *con la evaluación de la causa, la gestión y la evidencia de resolución."* *"La ticketera se creó el 6 de marzo de 2023 y se comenzó a utiliza el 2 de abril 2023, con el objeto de tener un registro de las gestiones que se realizan sobre el sistema de backup, en especial la resolución de los errores que puedan producirse en la ejecución diaria de los Jobs de backup.* *En La ticketera se reciben principalmente los errores/alertas que genera el sistema de Backup, y se cargan o reenvían los pedidos de los usuarios y las pruebas entre otros."*

La labor se desarrolló siguiendo los procedimientos y prácticas implementadas por esta Sindicatura General de la Nación según las Normas de Auditoría Interna Gubernamental (Resolución Nº 152/02-SGN). Se utilizaron como criterios las Normas Generales de Control Interno (Resolución Nº 172/2014-SGN) y las Normas de Control Interno para Tecnología de la

Información (Resolución Nº 87/22-SGN) aplicables para la auditoría de actividades de control relativas a la gestión de la tecnología informática.

Asimismo, se utilizó el plan de trabajo de esta Sindicatura para la verificación de los controles relacionados con el Plan de Resguardo y Recuperación de la Información, –ver Anexo-, siguiendo los criterios referidos a las mejores prácticas, entre ellas: ISO/IEC 27001 “Sistemas de Gestión de la Seguridad de la Información”, DA 641/2021 “Requisitos mínimos de Seguridad de la Información para Organismos", entre otras.

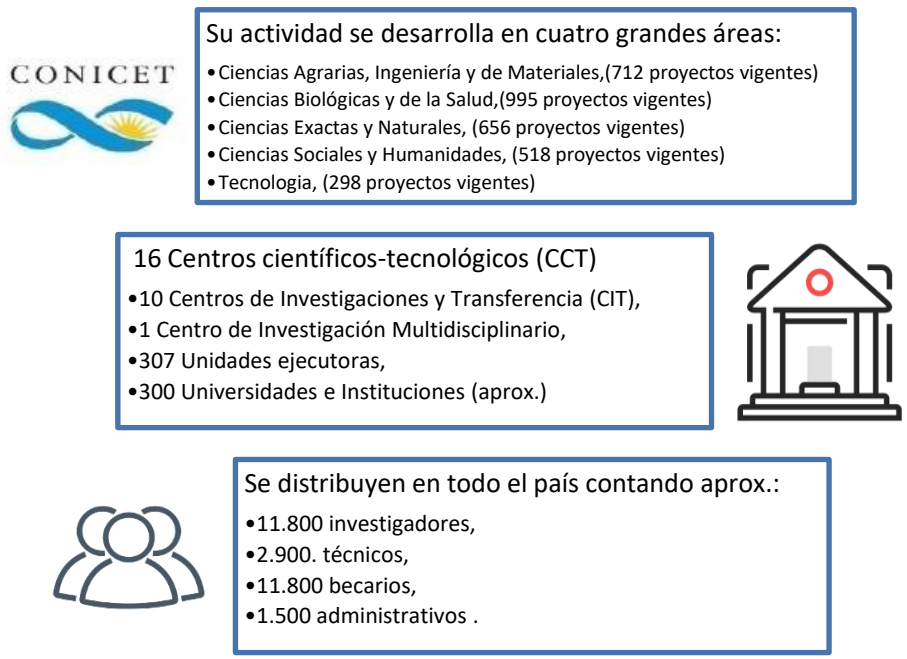
El presente informe se encuentra referido al estado de situación y las observaciones sobre el objetivo de la tarea hasta la fecha precedentemente indicada y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

4 MARCO DE REFERENCIA

El CONICET revista como ente autárquico del Estado Nacional bajo la órbita del Ministerio de Ciencia, Tecnología e Innovación (MinCyT).

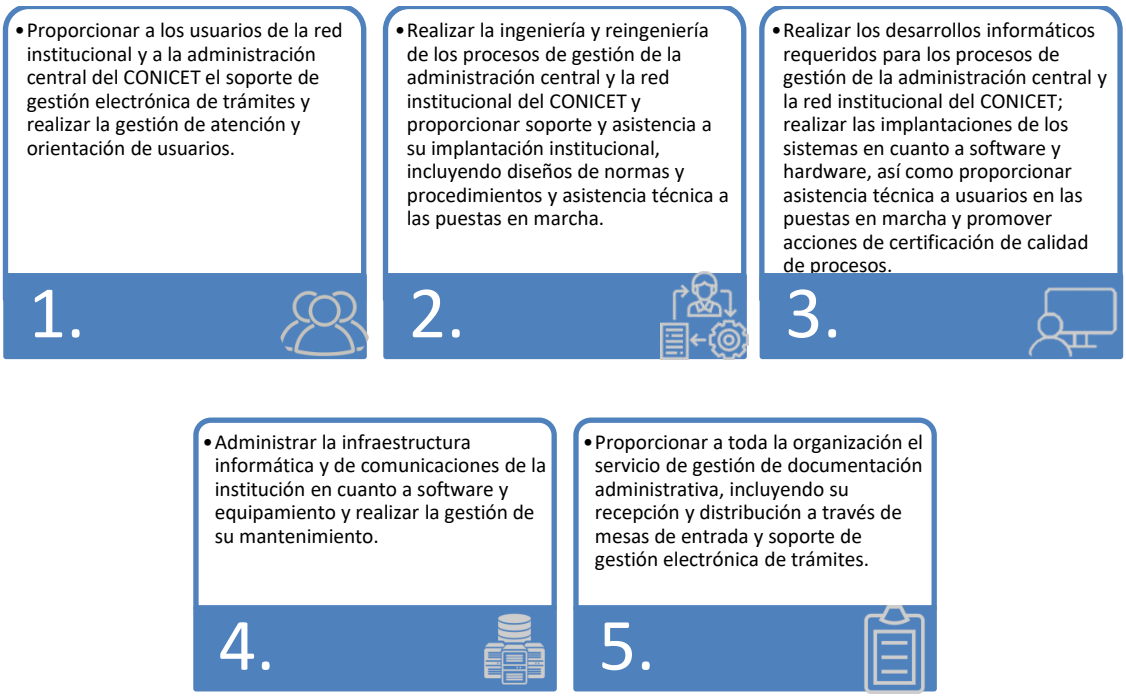
El CONICET fue creado por el Decreto Ley N° 1291 del 5 de febrero de 1958, y su misión es la promoción y ejecución de actividades científicas y tecnológicas en todo el territorio nacional y en las distintas áreas del conocimiento.

El siguiente gráfico expone las actividades que desarrolla en cuatro áreas el Organismo con sus proyectos vigentes[1], el volumen del personal y la cantidad de centros científico-tecnológicos que posee:



[1] Según lo publicado en el 2022, https://cifras.conicet.gov.ar/publica/

Según lo establece el Decreto N° 310/2007, las principales acciones de la Gerencia de Organización y Sistemas (en adelante, la GOS) son las siguientes:

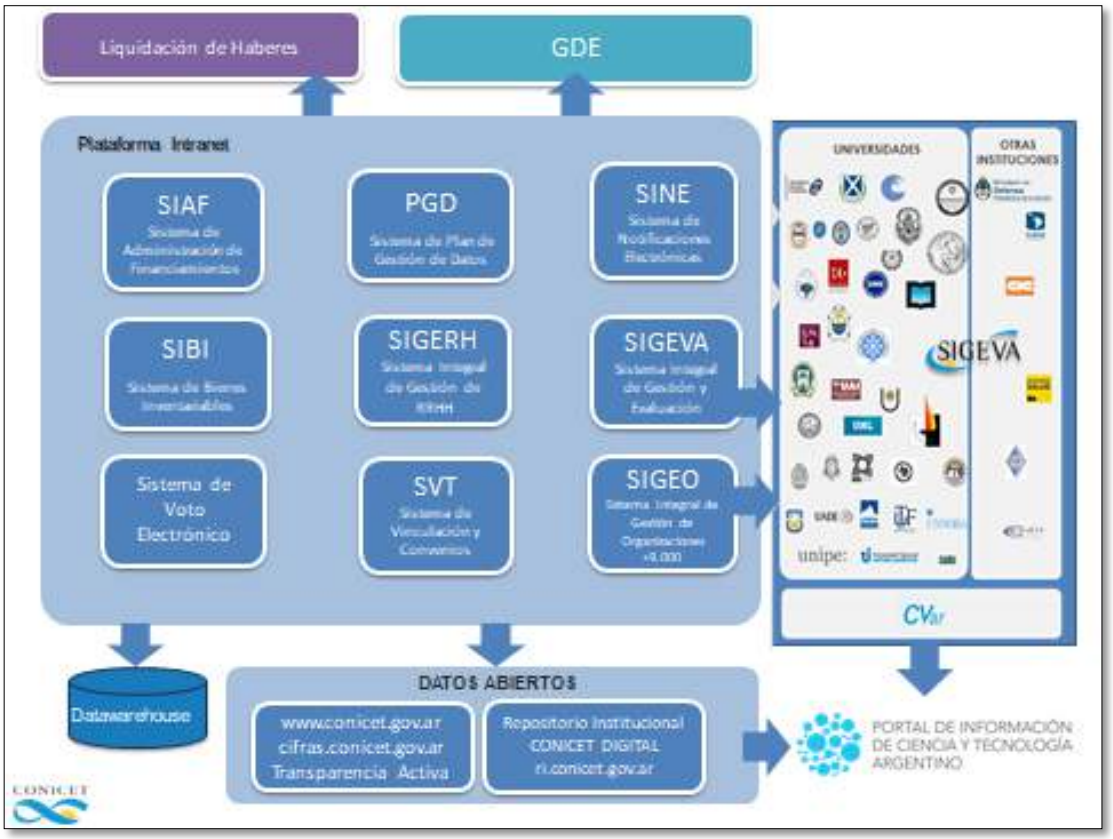


La GOS cuenta con 88 agentes de los cuales 19 prestan servicios en materia de TI en la ciudad de Tandil, ciudad donde el organismo posee un polo informático, en el cual trabajan 1.800 agentes aprox. La Oficina de Tecnología de la Información y Comunicaciones en Tandil (en adelante, OTIC Tandil) se encuentra activa desde el 01 de febrero de 2020.

Remitirse al punto 5.5 para más información al respecto.

4.1 SISTEMAS DE INFORMACIÓN DEL CONICET

A continuación, se presenta el esquema de interacción de los principales sistemas que son desarrollados y administrados por el CONICET para la gestión de ciencia y tecnología, el mismo se incluye en el "*Plan estratégico de TI 2023 – 2025.pdf*" provisto por el auditado.



Esquema de interacción de los principales sistemas

Se detallan las principales características de estos sistemas de información:

SISTEMA	DESCRIPCIÓN
1. **Sistema Informático de Administración de Financiamientos (SIAF)**	Sistema que permite la administración de los financiamientos otorgados por el CONICET y la rendición de cuentas de los mismos. Intervienen: **SIAF - Sistema Integral de Administración de Financiamientos** **SIAF-AGF - Autogestión de Fondos**
2. **Sistema Informático de Bienes Inventariables (SIBI)**	Sistema que permite llevar a cabo la administración patrimonial de los bienes en donde CONICET es considerado entidad beneficiaria. Permite el armado de los cargos patrimoniales por parte de las unidades divisionales, su procesamiento por el Departamento de Patrimonio, la generación de las etiquetas y la administración de los bienes. Realiza el cálculo de la amortización anual para todos los bienes registrados.
3. **Sistema Vinculación Tecnológica (SVT)**	Sistema que gestiona la oferta tecnológica, desde las demandas del sector como las posibles ofertas de los investigadores, así como su contratación, facturación y cobro de los servicios de transferencia. Cuenta con el seguimiento y control de los convenios firmados por el organismo con terceros.
4. **Plataforma INTRANET**	Es la plataforma que gestiona los usuarios y roles y la seguridad de las aplicaciones del CONICET.
5. **Sistema Integral de Notificaciones Electrónicas (SINE)**	Brinda una bandeja de entrada a todos los usuarios de Intranet para recibir por parte del organismo notificaciones y comunicaciones. Permite realizar estas notificaciones a través de los distintos sistemas del organismo y llevar un registro de lo ocurrido con las mismas.
6. **Sistema Integral de Gestión de Recursos Humanos (SIGERH)**	El sistema permite al personal de RRHH, gestionar toda la información referida al legajo de los agentes. El SIGERH mantiene una comunicación e intercambio de información con los distintos sistemas del CONICET.

SISTEMA	DESCRIPCIÓN
7. **Sistema Integral de Gestión de Organizaciones (SIGEO)**	Es un sistema de gestión de organizaciones que permite la gestión de información de éstas. Mantiene una comunicación e intercambio de información con los distintos sistemas del CONICET, como el SIGERH y a través de éste el Liquidador de Haberes, el SIGEVA, y la Intranet del organismo, entre otros.
8. **Sistema Integral de Gestión y Evaluación (SIGEVA)**	Realiza la gestión integral del proceso que permite la administración completa de las convocatorias e informes que se requieren presentar en el CONICET desde la presentación, hasta los procesos de gestión y control, evaluación y la decisión final en Directorio. Por otra parte, gestiona los Curriculum Vitae compatibles con el sistema CVar de todo el personal y becarios del CONICET, el banco de especialistas para las evaluaciones de pares y las interfaces con el repositorio de producción CyT, CONICET Digital.
9. **Repositorio Institucional CONICET Digital**	Es el Repositorio Institucional de acceso abierto del CONICET. Es una plataforma digital que pone a disposición de la sociedad, la producción científico-tecnológica del país. Este Repositorio se nutre del SIGEVA a través del cual investigadores, becarios y demás personal de CONICET autoarchivan su producción científico-tecnológica. Así, los metadatos y los trabajos publicados, con sus respectivos permisos y condiciones legales para su divulgación, son accesibles digitalmente desde este repositorio.
10. **Plan de Gestión de datos (PGD)**	Es la plataforma integrada a los demás sistemas del CONICET para contribuir a la planificación, organización y previsión de la colección digital de los datos recolectados, reutilizados o procesados en un proyecto de investigación financiado o cofinanciado por la Institución. La herramienta permite generar un plan de gestión de datos (PGD) abarcando el ciclo de vida completo del proyecto, desde la etapa de preparación de la propuesta hasta su terminación.
11. **Conicet en Cifras**	Herramienta para crear distintos tipos de gráficos interactivos que brinda información sobre el organismo tanto a usuarios internos (Directorio y Alta Gerencia) como a la comunidad externa en general (https://cifras.conicet.gov.ar/publica/). Esta herramienta se nutre de información de las diversas Gerencias del CONICET recolectada por varios de los sistemas de gestión y evaluación previamente mencionados.

Por otro lado, el gráfico especifica otros sistemas con los que se interactúa, pero que son desarrollados por terceros:

SISTEMA	DESCRIPCIÓN
12. **Liquidación de haberes TRAMIX**	Sistema, cuyo proveedor es UNITECH, y gestiona la liquidación de haberes del personal que trabaja para el CONICET así como otros organismos estatales. - Tramix Liquidación de Haberes - Integrador TramixLH - Sigerh Proveedor: UNITECH
13. **DATAWAREHOUSE**	Plataforma utilizada para recolectar y analizar datos provenientes de múltiples fuentes heterogéneas. Proveedor: Pentaho (Opensource)
14. **GDE**	Gestión Documental Electrónica. LUE: Legajo Único Electrónico.

Para más detalles sobre el Plan Estratégico de TI del CONICET y los sistemas informáticos del CONICET, remitirse al punto 5.6, 5.13 y 5.14 respectivamente.

4.2 CPD PRINCIPAL EN CONICET CENTRAL

El CONICET cuenta con un CPD Principal donde procesa sus sistemas y servicios, el mismo se encuentra ubicado en el octavo piso del CONICET CENTRAL, en Godoy Cruz 2290, CABA, en una de las instalaciones que forman parte del Polo Científico-Tecnológico[2].

De la visita al CPD Principal, se enlistan los principales mecanismos de control implementados:

Control de Accesos: cuentan con un sistema informático de control de accesos, control biométrico y llevan un registro de visitantes.

El sistema de control de accesos (edificio, cocheras, oficinas, CPD, etc.) es gestionado por el MINCyT, debido a que depende y se ubica en el Polo Científico Tecnológico.

El resultado de la verificación de los usuarios que acceden al CPD Principal se encuentra en el punto 5.4.

A su vez, poseen implementado un CCTV (Circuito Cerrado de Televisión).

Acceso biométrico - CCTV

Sistema de refrigeración: los racks del CPD cuentan con un sistema de refrigeración integral que mantiene una temperatura estable de +- 20°C. Asimismo, el CPD cuenta con un sistema de respaldo en caso de fallas compuesto por 2 aires acondicionados:

Refrigeración en racks

[2] Conjunto de edificios que funciona como sede de diferentes instituciones relacionadas con la ciencia y la tecnología

Sistema de respaldo de refrigeración

Aspectos generales: se observa piso técnico, canaletas ignífugas y cableado acorde a las normas de seguridad.

Piso técnico

Canaletas ignífugas

Cableado

Sensores y detectores preventivos: se encuentran instalados sensores de humo, humedad, temperatura, detectores de incendios, los que ante alguna anomalía emiten alertas al personal correspondiente.

Sensores

Alarma incendios

Sistema de contención de incendios automático: ante un incendio, cuentan con un sistema que libera un gas presurizado que extingue los posibles incendios, así como matafuegos y alarmas de incendios.

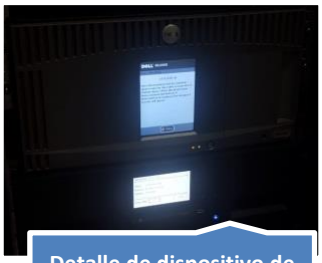
Sistema de detección de incencios

Dispositivos de Resguardo. A continuación, se enumeran los equipos verificados y las tareas que efectúan:

- Copia a disco en un equipo dedicado para el resguardo (Raid 5).
- Copia a disco dentro del dispositivo de almacenamiento/storage (Dell/IBM) que no son extraíbles y quedan dentro del CPD Principal.
- Cintas obsoletas: cuentan con un dispositivo para recuperar las cintas obsoletas LTO-5.

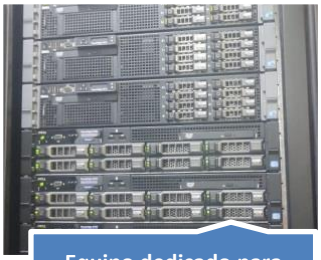
Dispositivo de almacenamiento/storage dell

Dispositivo en cintas LTO actuales



Detalle de dispositivo de cinta actuales

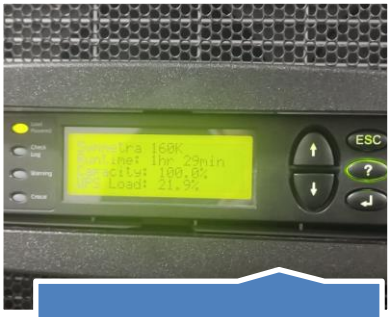
Dispositivos de cinta LTO - 05 obsoletos



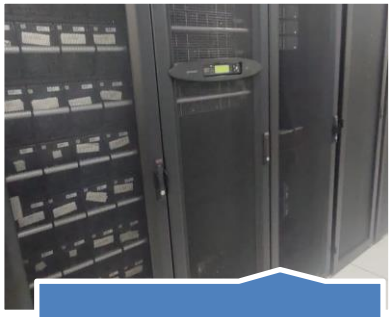
Equipo dedicado para resguardo RAID 5

Energía Eléctrica y UPS: posee un tablero de control y monitoreo instalado en un lugar visible, accesible, cerca de la salida del CPD.

Por otro lado, el UPS se encuentra en los primeros 3 racks dentro del CPD. Según lo informado, el grupo electrógeno no lo gestiona el CONICET, sino el MINCyT, que se localiza también en el Polo Científico Tecnológico.



Tablero del UPS



Rack de UPS

Para tomar conocimiento acerca de las debilidades encontradas en materia de seguridad física del CPD Principal, remitirse al punto 5.4.

4.3 CONSIDERACIONES GENERALES DEL PROCESO DE RESGUARDO Y RECUPERACIÓN

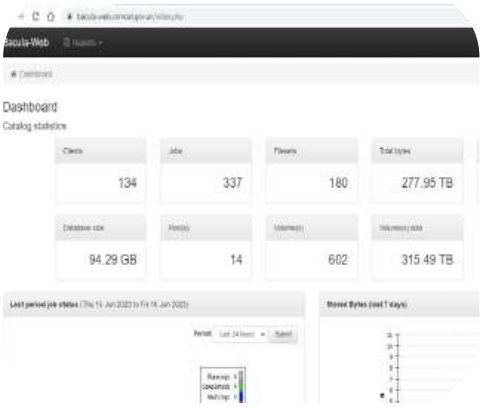
4.3.1 SISTEMA DE GESTIÓN DE RESGUARDO Y RECUPERACIÓN DE LA INFORMACIÓN

BACULA (https://www.baculasystems.com/es) es un sistema informático opensource elegido por CONICET para administrar resguardos (copias de seguridad) y recuperación de todos los datos a resguardar.

El sistema lleva un registro de todas las ejecuciones (resguardo / recuperación) exitosas o no y permite gestionar los errores así como registrar su resolución. Asimismo, concentra todos los archivos y directorios procesados e incluidos en cada ejecución.

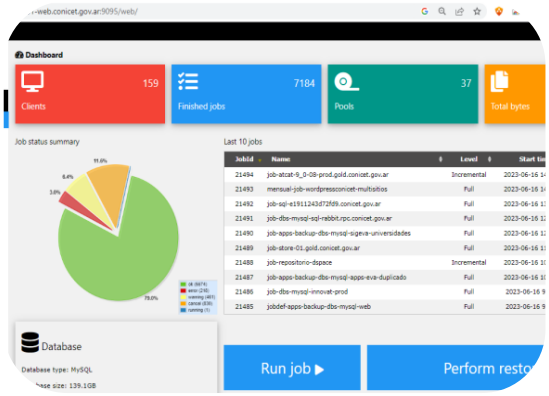
Reside en un servidor Linux (Ubuntu, versión 20.04) y utiliza una base de datos en MySql versión 8.0.33.

Como antecedente y debido al cambio tecnológico, el CONICET posee dos versiones de BACULA instaladas:



En 2016 hasta septiembre 2022 se utilizó la primera versión de Bacula. En esta versión, si un Job arrojaba errores, quedaba el aviso en un correo electrónico o manualmente se cargaba un ticket de soporte general. Los logs se registraban y resguardaban dentro del mismo Bacula.

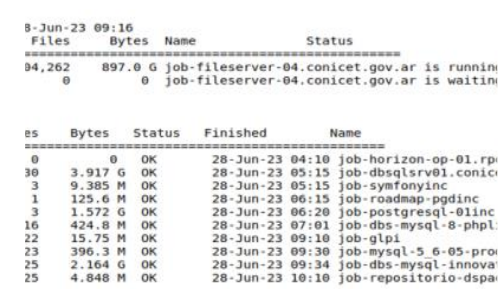
Se encuentran registrados 96.287 Jobs según documento *"BACULA conicet ANTERIOR.docx".*



En julio 2022, se implementó la última versión del sistema que demandaba nuevo hardware para gestionar los resguardos. Según lo informado, los Jobs antiguos fueron migrados. Actualmente, cada vez que un job no se finaliza por cualquier motivo, automáticamente se abre un ticket en la ticketera denominada "OTRS" y un técnico debe tomarlo, analizarlo y cerrarlo.

El sistema cuenta con dos interfaces de acceso:

BACULA - Interfaces de acceso



```
8-Jun-23 09:16
 Files     Bytes  Name                Status
==========================================
94,262    897.0 G job-fileserver-04.conicet.gov.ar is runnin
     0          0 job-fileserver-04.conicet.gov.ar is waitin


es    Bytes   Status   Finished        Name
=============================================
 0        0   OK       28-Jun-23 04:10 job-horizon-op-01.rp
30    3.917 G OK       28-Jun-23 05:15 job-dbsqlsrv01.conic
 3    9.385 M OK       28-Jun-23 05:15 job-symfonyinc
 1    125.6 M OK       28-Jun-23 06:15 job-roadmap-pgdinc
 3    1.572 G OK       28-Jun-23 06:20 job-postgresql-01inc
16    424.8 M OK       28-Jun-23 07:01 job-dbs-mysql-8-phpl
22    15.75 M OK       28-Jun-23 09:10 job-glpi
23    396.3 M OK       28-Jun-23 09:30 job-mysql-5_6-05-pro
25    2.164 G OK       28-Jun-23 09:34 job-dbs-mysql-innova
25    4.848 M OK       28-Jun-23 10:10 job-repositorio-dspa
```

Bconsole:

Acceso vía línea de comandos

Permite ver el estado de todos los dispositivos de Almacenamiento/Storage, sean discos o bien cintas LTO.

Baculum:

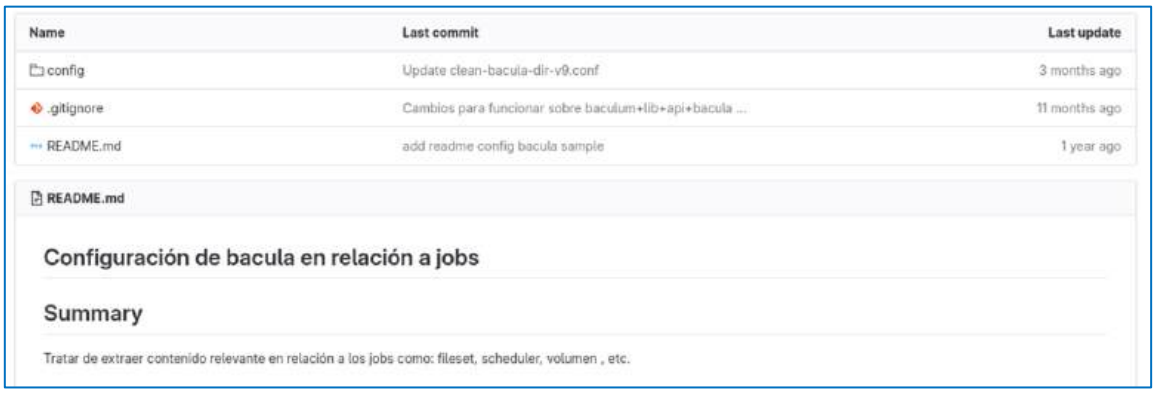
Acceso vía web

Permite configurar y administrar Bacula, visualizar estadísticas de uso, interactuar con Bconsole y configurar usuarios.

4.3.2 REPOSITORIO DE JOBS

Para poder conservar todo lo relacionado a la implementación, configuración y Jobs asociados, se mantiene el repositorio "BACULA" en GitLab, la

herramienta de control de versiones oficial de CONICET. Se adjunta la captura, provista por el auditado.



4.3.3 SITIO EXTERNO DE CINTAS DE RESGUARDO - ARCHIVO INSTITUCIONAL DEL CONICET

Las cintas que están designadas con el fin de resguardar la información en un sitio externo, son **externalizadas al Archivo Institucional del CONICET** (en adelante, el Archivo), **sede Rivadavia 1917, Primer Piso.**

De la visita al Archivo, se enlistan los principales mecanismos de control implementados:

- El edificio donde se encuentra el Archivo, cuenta con una Mesa de Entrada que constata la identidad de los visitantes.
- El Archivo contiene la caja fuerte ignífuga donde se ubican las copias de seguridad en cinta de los resguardos mensuales full.
- Por último, en el siguiente gráfico se exponen las medidas de seguridad del Archivo:

Molinete Sede

Aires Acondicionado

Puerta de acceso al Archivo

Camaras de seguridad

Sensor de humo

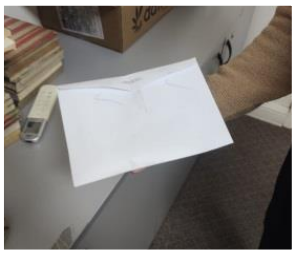
Exitintor de incendio

Alarma de incencio

Luces de emergencia

Caja fuerte ignífuga

Armario Resguardo de llave para caja fuerte.



Llave ensobrada

Para tomar conocimiento acerca de las debilidades encontradas en materia de seguridad física del Archivo, remitirse al punto 5.4.

4.3.4 RESPONSABLES Y ACTORES DEL PROCESO DE RESGUARDO Y RECUPERACIÓN

Se enlistan los principales actores del proceso, que surgen del relevamiento efectuado:

- **Equipo de Resguardo:** revisa diariamente la ticketera de resguardo para verificar su ejecución. Si el resultado de la verificación arroja alertas las resuelve y si excede su competencia las deriva.

- **Responsable de Seguridad de la Información** verifica las tareas de resguardo y de encontrarse errores o faltantes de información, informa al Operador de Resguardo y Restauración para que corrija los errores y vuelva a ejecutar las pruebas.

- **Responsable de Resguardo y Restauración:** define el estándar de resguardo y restauración, genera los planes de respaldos, coordina, ejecuta y verifica los resguardos de información y lleva registros de las ejecuciones y sus contenidos. Planifica y ejecuta las pruebas de restauración y lleva registro de los resultados de las pruebas. Autoriza las solicitudes de respaldo especiales.

- **Responsable del Activo de Información:** persona que determina la criticidad de la información que se encuentra bajo su custodia.

- **Responsable Técnico del Activo de Información:** tiene conocimiento técnico del activo de información asociado a la estructura de datos a resguardar y la arquitectura de sistemas. Es responsable de definir los ítems a resguardar, su tamaño aproximado, el servicio prestado y el tipo de servicio.

- **Requirente/Solicitante:** persona autorizada que requiere recuperar datos resguardados, o bien solicita resguardar otra información que no se encuentre resguardada.

- **Responsable de Archivo:** recibe/remite el maletín estanco con las cintas a resguardar/recuperar.

- **Servicios Generales CONICET Central:** área que gestiona el traslado seguro entre ambas sedes (Conicet Central – Archivo Institucional).

Para tomar conocimiento acerca de los roles y funciones del área de TI del Organismo, remitirse al punto 5.5.

5 OBSERVACIONES, OPINIÓN DEL AUDITADO Y COMENTARIO FINAL DE SIGEN

Para la presente labor de auditoría se enlistan a continuación los principales reportes provistos por el auditado, detallados en el punto 3, los cuales fueron utilizados para distintos análisis y pruebas durante esta auditoría:

1. ***Jobs + Externalizaciones.xlsx:*** planilla de cálculo que detalla las tareas de resguardo (Jobs) ejecutadas en el mes de junio del corriente. Contiene la siguiente información:

    a. ***Solapa 1: Reporte "Junio TODO Cinta y Disco"***
        - Detalle de todos los Jobs ejecutados en el mes de junio 2023.

    b. **Solapa 2: Reporte "Junio SOLO Externalizado"**
        - Detalle de las cintas que se resguardan en sitio externo.

    c. ***Solapa 3: Reporte "Cintas Externalizadas TODAS"***
        - Reporte que acompañan las cintas en sitio externo.

2. ***BACULA.log.2.gz:*** registro de logs de las tareas de resguardo (Jobs) ejecutadas en el mes de junio del corriente.

3. ***JobsEnabled20230811.xlsx:*** listado de las tareas de resguardo (universo de Jobs).

4. ***SERVIDORES - Hostnames.xlsx:*** inventario de activos de información, el cual se encuentra en proceso de elaboración, que describe Jobs, servidores y servicios asociados, entre otros.

5. ***Reporte_Backup.xslx:*** universo de incidentes desde marzo a junio.

A continuación, se exponen las observaciones surgidas durante el trabajo llevado a cabo por esta Sindicatura.

5.1 POLÍTICA Y PROCEDIMIENTO DE RESGUARDO Y RECUPERACIÓN DE LA INFORMACIÓN

El organismo cuenta con una *"Política de Resguardo y Recuperación De Información.pdf*", de fecha 22 de mayo del corriente.

Durante el transcurso de esta labor, esta política fue elaborada y aprobada por el Directorio (IF-2023-61029162-APN-GOYS#CONICET), mediante el memo ME-2023-66480202-APN-CONICET#MCT de fecha 7 de junio de 2023.

En línea con dicha política, se recibió el **procedimiento** denominado "*Manual de Procesos MP-GOS-DGUyR-001 - del Resguardo/Backup a la Restauración.pdf*" de fecha 12 de abril de 2023, el cual **no se encuentra aprobado por la autoridad.**

Tanto la política aprobada como el procedimiento borrador remitido especifican los datos a resguardar: "*Datos en formato digital y software que conforman un servicio TI de valor para el Organismo, así como todo el material de apoyo necesario para procesar la información (documentos, base de datos, archivos de registro, programas, archivos de configuración - de software y hardware-, controladores o drivers, archivos de instalación, sistemas operativos y demás software de base, entre otros).*"

Según lo informado por el auditado, **el procedimiento** borrador representaría la gestión de resguardo y recuperación de la información que tienen planificada, sin embargo, **aún no refleja la práctica actual.**

El auditado ha elaborado una presentación *("Presentación Jornada Sigen.pptx")* con el fin de que esta Sindicatura tome conocimiento acerca de la práctica actual de la gestión de resguardo y recuperación de la información.

En los puntos 5.2 y 5.3, se detalla la práctica actual informal sobre esta gestión, la cual surge del relevamiento llevado a cabo, de la presentación que nos fue proporcionada y del resto de la documentación remitida.

Recomendación

Dado que el procedimiento de resguardo de recuperación de la información se encuentra pendiente de aprobación, considerar e incorporar los aspectos de control referente a las debilidades identificadas en la presente auditoría a modo de concluir con el procedimiento e implementarlo. Gestionar su aprobación formal por la autoridad.

El procedimiento debe asegurar no solamente la disponibilidad de la información en forma oportuna, sino también la integridad de los datos resguardados.

Se sugiere considerar la guía "Plan de Resguardo y Recuperación de la información", que se adjunta como Anexo.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"Al momento de recibir el informe el procedimiento "MP-GOS-DGUyR-001 – del Resguardo/Backup a la Restauración" se encuentra en proceso de aprobación por lo que las recomendaciones serán tenidas en cuenta para la próxima revisión del documento."

Descripción del Curso de Acción a Seguir:
"En la próxima revisión del procedimiento, contemplar aquellas recomendaciones pertinentes expuestas en el anexo del informe "Plan de Resguardo y Recuperación de la información."

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: *"Responsable de Seg. Inf + Dirección de Ingeniería de Procesos."*

Comentario final SIGEN

El comentario del auditado prevé recoger lo recomendado en el punto. No se efectúan comentarios adicionales.

5.2 DETALLES SOBRE LA PRÁCTICA ACTUAL DE RESGUARDO DE LA INFORMACIÓN

5.2.1 Inventariar activos de información relativos a los servicios y sistemas

El **procedimiento borrador** "*Manual de Procesos MP-GOS-DGUyR-001 - del Resguardo/Backup a la Restauración.pdf*", menciona que los activos de información deben concentrarse en un inventario a cargo del Responsable de Infraestructura y del Responsable Técnico del activo, sin embargo, en la actualidad, **este inventario se encuentra en etapa de elaboración** por parte de la GOS.

El auditado ha remitido una planilla de cálculo que contiene el inventario en elaboración *"SERVIDORES – Hostnames.xlsx".* Esta planilla de cálculo se compone de las siguientes solapas que se registran manualmente: Servidores, Jobs BACULA, Servidor - Job, Job-Servicio, Ids Jobs BACULA, Cruce.

De acuerdo al procedimiento borrador, el inventario debe contemplar la siguiente información:

- *"Identificación del equipo físico o virtual*
- *Servicio prestado por el/los equipo/s*
- *Nombre del Activo/Sistema/Descripción*
- *Tipo de servicio / Stack Tecnológico*[3]
- *Ubicación lógica del conjunto de archivos a resguardar (fileset)*
- *Tamaño aproximado de los datos a resguardar".*

Sin embargo, el inventario en elaboración **no contempla los ítems enumerados**.

Por otro lado, se verificó que **no se registra la participación del propietario de los activos de información.**

[3] Listado de todos los servicios tecnológicos, sistemas, herramientas y componentes utilizados para crear y ejecutar una aplicación. Incluye lenguajes de programación, bases de datos, bibliotecas, frameworks y herramientas de desarrollo, entre otros.)

5.2 2 Clasificar los datos y definir el resguardo

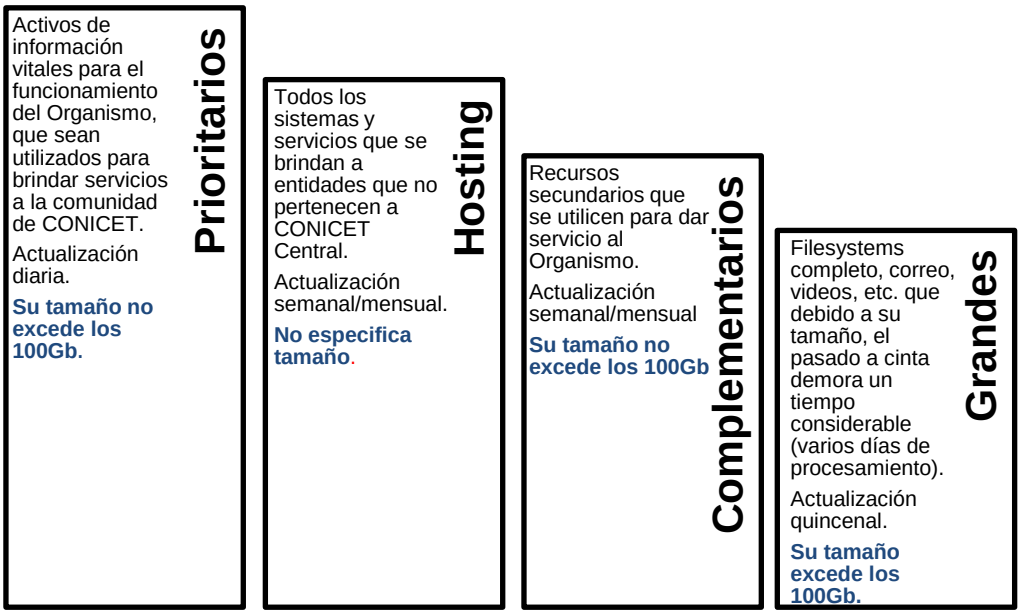
La **definición de la criticidad de los datos a resguardar** (sistemas/servicios críticos), **se encuentra en proceso actualmente**. Cabe resaltar que esta tarea está siendo realizada **sin ninguna metodología.**

En el mismo orden, el auditado ha remitido el **documento sin aprobación,** *"Criterios de clasificación de los activos a resguardar.docx",* del cual se desprenden las siguientes particularidades:

- El objetivo del documento es ordenar y establecer un criterio para el resguardo de la información del organismo en medios extraíbles (cintas y en disco) para poseer, por lo menos, una (1) copia mensual de toda la información y poder luego guardar dicha copia en un lugar externo, en el Archivo Institucional del Organismo, ubicado en Rivadavia 1917.

- El documento especifica que cada tarea de resguardo (en adelante, Jobs) que se programa se encuentre dentro de una categoría a modo de determinar estrategias diferenciadas de resguardo. Cada categoría propone una prioridad, una metodologías de resguardo diferente (a disco, cinta // incremental, diferencial y completo), periodicidad, tamaño, y una descripción de los activos de información a resguardar.

Se exponen seguidamente los 4 grupos descriptos en el documento borrador analizado, por orden de prioridad de resguardo, según el análisis efectuado sobre el mismo:



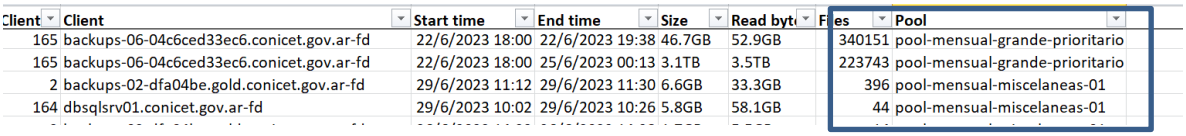
Cabe destacar que este **documento resulta poco claro dado que no especifica en forma ordenada y para cada grupo, la prioridad, actualización, tamaño y qué grupo debe resguardarse en el sitio externo.**

Por otro lado, de acuerdo a los reportes de resguardos extraídos del BACULA **se puede observar la existencia de un grupo adicional denominado:**

Misceláneas- 0.1, que **no se encuentra incluido en el documento borrador bajo análisis y del cual se desconoce el tipo de información qué resguarda, su prioridad, actualización, tamaño y si se trata de información que debe resguardarse en sitio externo, en forma mensual. Por otro lado, en BACULA están agrupados los Jobs en "Grandes-Prioritarios".**

Se adjuntan extractos de reportes de BACULA, a modo de ejemplo.

Reporte BACULA: Jobs + Externalizacion.xlsx:



Client	Client	Start time	End time	Size	Read byt	Files	Pool
165	backups-06-04c6ced33ec6.conicet.gov.ar-fd	22/6/2023 18:00	22/6/2023 19:38	46.7GB	52.9GB	340151	pool-mensual-grande-prioritario
165	backups-06-04c6ced33ec6.conicet.gov.ar-fd	22/6/2023 18:00	25/6/2023 00:13	3.1TB	3.5TB	223743	pool-mensual-grande-prioritario
2	backups-02-dfa04be.gold.conicet.gov.ar-fd	29/6/2023 11:12	29/6/2023 11:30	6.6GB	33.3GB	396	pool-mensual-miscelaneas-01
164	dbsqlsrv01.conicet.gov.ar-fd	29/6/2023 10:02	29/6/2023 10:26	5.8GB	58.1GB	44	pool-mensual-miscelaneas-01

Por lo relevado, surgen las siguientes debilidades:

- **La definición de la criticidad de los datos a resguardar (sistemas/servicios críticos) está siendo realizada sin una metodología.**

- **El documento resulta poco claro dado que no especifica en forma ordenada los grupos, su prioridad, actualización, su tamaño de las tareas de resguardo de los sistemas y servicios, y además, no incluye el grupo "*Misceláneas- 0.1.***

- **El documento bajo análisis "***"Criterios de clasificación de los activos a resguardar.docx*"**, se encuentra sin aprobar.**

5.2.3 Programar los Jobs

El Responsable de Resguardo y Restauración programa las tareas de resguardo en BACULA considerando los tipos de medios de almacenamiento (cinta/disco) utilizados por CONICET, según un cronograma (diario, semanal y quincenal/full, diferencial e incremental) que se menciona en el documento borrador visto en el punto anterior *"Criterios de clasificación de los activos a resguardar.docx*". También se configuran los pool de almacenamiento, rotulaciones y reutilización entre otras cuestiones.

Se solicitó el universo de Jobs programados desde enero del corriente hasta la fecha, habiéndose recibido el reporte *"JobsEnabled20230811.xlsx",* que contiene únicamente los nombres de 206 Jobs a julio 2023, con lo cual **no se pudo tomar conocimiento sobre el número o id de Job.**

Por otro, surge por el archivo *"Jobs + Externalizacion.xslx"*, que se utilizaron en junio del corriente 245 Jobs.

Como resultado del cruce de Jobs entre ambos documentos surge que:

- Se verifica la existencia de **40 Jobs** adicionales en el reporte *"Jobs + Externalizacion.xslx"*, es decir, que fueron ejecutados en junio del 2023

pero no existen en el universo de Jobs programados, provisto por el auditado.

- En el reporte de los Jobs ejecutados en junio del corriente en el sistema BACULA *("Jobs + Externalizaciones.xslx")* no es posible determinar para cada uno de los Jobs programados qué sistema/servicio/datos resguarda.

De acuerdo a lo informado por el auditado, **los números encontrados en el campo "Job ID" no corresponden a un identificador único de un Job sino que corresponde a su ejecución (entiéndase, que pueden ejecutarse múltiples veces cada Job).**

5.2.4 Rotulación y reutilización de medios de almacenamiento

Si bien la *"Política de Resguardo y Recuperación De Información.pdf"* aprobada contempla ciertos aspectos y lineamientos referentes a la rotulación y reutilización de medios de almacenamiento, **no se encuentran suficientemente definidos en el procedimiento borrador** "*Manual de Procesos MP-GOS-DGUyR-001 - del Resguardo/Backup a la Restauración.pdf*" ni en algún otro documento formal.

5.2.5 Ejecutar el proceso de resguardo

Según lo relevado, los procesos de resguardo, es decir los Jobs, se ejecutan tal como fueron configurados en BACULA, se realizan las verificaciones correspondientes a los resultados de su ejecución y se corrigen errores, de existir, por parte del Responsable de resguardo y restauración, haciendo uso de una herramienta de gestión de tickets denominada OTRS.

Mensualmente, el área de Seguridad de la Información emite reportes desde BACULA acerca de los resguardos ejecutados: *Resumen de ejecuciones, Ejecuciones totales del mes, Ejecuciones de los últimos meses, entre otros*. Estos datos se extraen desde BACULA.

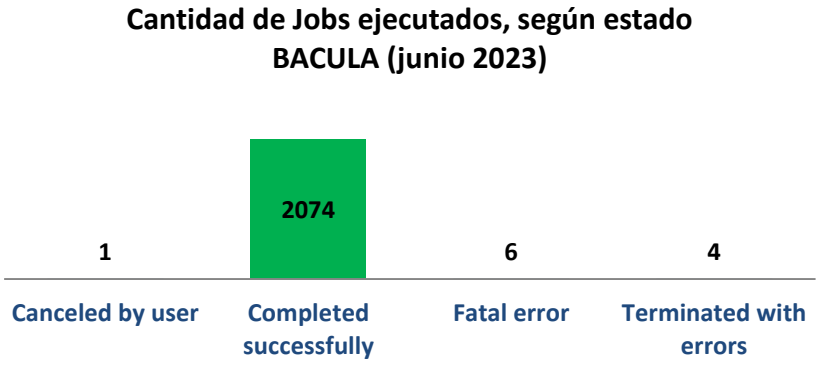
El auditado ha proporcionado el reporte *"Jobs + Externalizacion.xlsx*" referente al reporte de resguardo ejecutados en el mes de junio del corriente, a fin de verificar el procedimiento de resguardo implementado.

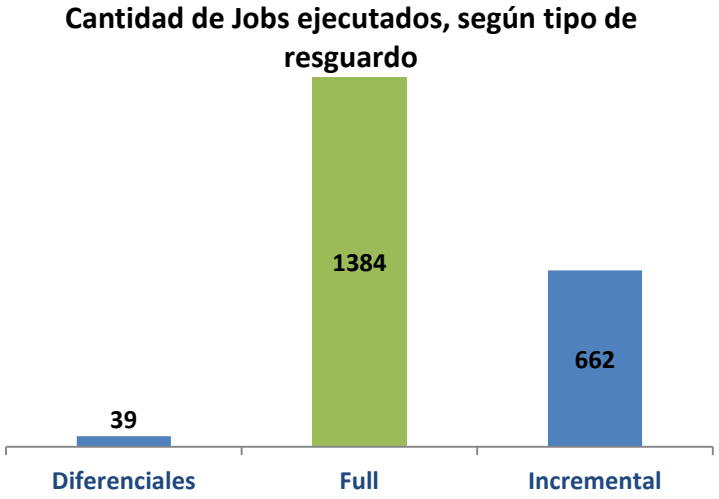
El reporte está compuesto por 3 solapas: *Solapa 1: Reporte "Junio TODO Cinta y Disco", Solapa 2: Reporte "Junio SOLO Externalizado"* y *Solapa 3: Reporte "Cintas Externalizadas TODAS".*

La Solapa 1 contiene los datos sobre los atributos de los Jobs ejecutados en junio 2023, como ser: ID, nombre, nivel o tipo de resguardo (diferencial, full, incremental), cuando se ejecuta y termina, su estado, el tamaño de su ejecución, el id del Pool, el nombre del pool, el tamaño, entre otros datos.

De este reporte surge:

- 2085 Jobs ejecutados en junio 2023 (diferenciales, full, incremental), según los 4 estados que maneja BACULA:





- Se identificaron 245 Jobs programados en BACULA que se utilizaron en el mes bajo análisis.

- Las cintas, con tipo de resguardo FULL, que se destinan a almacenarse en sitio externo se denominan “pool-mensual-grande-prioritario” y ”pool-mensual-miscelaneas-01”

“pool-mensual-grande-prioritario”: 152 Jobs (15,64 TB)
“pool-mensual-miscelaneas-01”: 17 Jobs (1,73 TB)

Durante el mes de junio se ejecutaron 169 Jobs full en cinta (LTO) para externalización por un total de 17,35TB.

Registro de logs

Según la política *“Política de Resguardo y Recuperación De Información.pdf”* el proceso de copia de seguridad debe generar un registro de ejecución u operación (log) que permita la revisión del resultado de la ejecución.

A modo de verificar que los Jobs ejecutados en el mes de junio 2023 han sido adecuadamente registrados en el log por parte de BACULA, el auditado ha remitido el archivo *"BACULA.log.2.gz",* mediante el cual se pudo verificar que BACULA ha registrado los 2085 Jobs ejecutados en ese mes (según el reporte *"Jobs + Externalizacion.xlsx").*

Para verificar que los logs registren todos los datos de los campos claves en la operatoria, se tomó el único Job cuyo estado fue *"Canceled by user" en el reporte "Jobs + Externalizacion.xlsx"* y se lo buscó por número de ejecución del Job (20891) en el registro de log que generó BACULA.

JobI	Name	Lev	SchedTime	StartTime	EndTime	Tiemp	JobSta	Estado
20891	job-fileserver-01.conicet.gov.ar	F	5/6/2023 21:41	5/6/2023 21:41	5/6/2023 22:12	00:30:44	A	Canceled by user

Como se puede observar en el log, el **estado no coincide** (se registró en el log como "Backup Canceled") y además, **no registra el usuario que efectuó esta cancelación.**

```
05-Jun 21:41 baculadirector-dir JobId 20891: Start Backup JobId 20891, Job=job-
fileserver-01.conicet.gov.ar.2023-06-05_21.41.43_40
05-Jun 21:41 baculadirector-dir JobId 20891: Using Device "drive-ibm-1" to write.
05-Jun 21:41 fileserver-01.conicet.gov.ar-fd JobId 20891: Generate VSS snapshots.
Driver="Win64 VSS"
05-Jun 21:41 fileserver-01.conicet.gov.ar-fd JobId 20891:     Snapshot mount point: E:\
05-Jun 22:12 baculadirector-dir JobId 20891: Bacula baculadirector-dir 9.4.2 (04Feb19):
  Build OS:               x86_64-pc-linux-gnu ubuntu 20.04
  JobId:                  20891
  Job:                    job-fileserver-01.conicet.gov.ar.2023-06-05_21.41.43_40
  Backup Level:           Full
  Client:                 "fileserver-01.conicet.gov.ar-fd" 9.4.2 (04Feb19) Microsoft
Standard Edition (build 9200), 64-bit,Cross-compile,Win64
  FileSet:                "FileSet-fileserver-01.conicet.gov.ar" 2022-08-05 11:03:41
  Pool:                   "pool-mensual-grande-prioritario" (From Job resource)
  Catalog:                "MyCatalog" (From Client resource)
  Storage:                "storage-library-talio-part1-sd" (From Pool resource)
  Scheduled time:         05-Jun-2023 21:41:41
  Start time:             05-Jun-2023 21:41:43
  End time:               05-Jun-2023 22:12:27
  Elapsed time:           30 mins 44 secs
  Priority:               10
  FD Files Written:       53,716
  SD Files Written:       0
  FD Bytes Written:       25,934,610,531 (25.93 GB)
  SD Bytes Written:       0 (0 B)
  Rate:                   14064.3 KB/s
  Software Compression:   None
  Comm Line Compression:  None
  Snapshot/VSS:           no
  Encryption:             no
  Accurate:               no
  Volume name(s):
  Volume Session Id:      187
  Volume Session Time:    1683640816
  Last Volume Bytes:      3,262,655,821,824 (3.262 TB)
  Non-fatal FD errors:    0
  SD Errors:              0
  FD termination status:  Canceled
  SD termination status:  Canceled
  Termination:            Backup Canceled
```

Adicionalmente, **no se pudo identificar el incidente asociado a esta cancelación y su causa** en el *"Reporte_Backup.xlxs"*- que contiene el total de incidentes cargados en la herramienta de tickets "OTRS" desde marzo a junio del corriente, debido a que no incluye el número de ejecución del Job**.** Este reporte fue analizado en profundidad en el punto 5.2.7.

Por lo expuesto surgen las siguientes debilidades:

- **No se pudo verificar qué usuario fue el que efectuó esta acción en BACULA, lo cual denota conflictos de trazabilidad en las operaciones efectuadas.**

- **Discrepancia en los estados configurados en BACULA, reportes y registro de log.**

- **En el reporte de incidentes *"Reporte_Backup.xlxs"*, tampoco fue posible efectuar trazabilidad, debido a que no se pudo verificar el registro de incidente asociado a esta cancelación.**

- **De los archivos analizados, no se pudo identificar la causa por la cual el Job fue cancelado.**

5.2.6 Externalizar el resguardo de las cintas que correspondan

Mensualmente, se procede a externalizar los resguardos full en cinta.

- Para ello, el Responsable de Resguardo y Restauración extrae las cintas que corresponden del dispositivo de almacenamiento del CPD Principal.

    - Este dispositivo tiene la capacidad para gestionar 80 cintas y permite reciclar las cintas automáticamente.

- Luego, rotula las cintas manualmente y prepara los reportes con el listado de Jobs almacenados en las mismas y el detalle de las cintas enviadas a Archivo (para poder hacer una búsqueda manual en caso de requerirse- si no se contara con la información del sistema de resguardo).

- Personal autorizado del área Servicios Generales del CONICET Central traslada en un maletín estanco las cintas junto con el listado de Jobs y asimismo, lleva el remito al Archivo Institucional, allí el Responsable del Archivo firma el remito y da aviso de recepción a través de un ticket al alias backup@conicet.gov.ar con Asunto "Recepción de Cintas Nro. X".

Para verificar el proceso de externalización de las cintas del mes de junio 2023, se consideró el reporte "*Jobs + Externalizaciones.xlsx: Solapa 2: "Junio SOLO Externalizado" y Solapa 3: "Cintas Externalizadas TODAS.xlsx".*

- ***Solapa 2: "Junio SOLO Externalizado"***

Este reporte contiene el detalle de los Jobs ejecutados de los grupos *"Grande – Prioritario"* y "*Misceláneas-01*" (resguardos Jobs full en cintas que se destinan a Archivo).

- **Grande-prioritario:** Total Jobs: 17 (modo full)

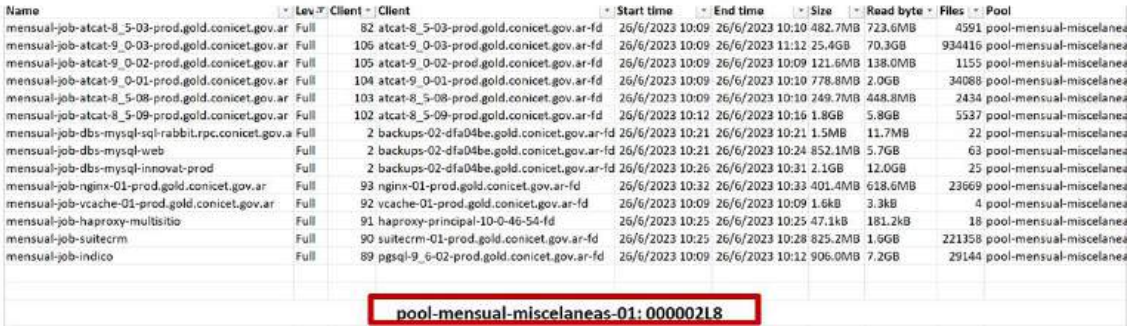
    - pool-mensual-grande-prioritario: 000007L8, 000013L8

- **Miscelaneas-01:** Total Jobs: 151 (modo full)
  - pool-mensual-misceláneas-01: 000002L8

Se reitera que el grupo ***Miscelaneas-01*** **no se encuentra definido y además se observa que el grupo *"grande-prioritario"* son tratados como categorías independientes en el documento borrador remitido *"Criterios de clasificación de los activos a resguardar.docx".***

JobId	Name	Level	ClientId	Client	Start time	End time	Size	Read bytes	Files	Pool
#####	job-fileserver-04.conicet.gov.ar	Full	162	fileserver-04.conicet.gov.ar-fd	27/6/2023 18:30	29/6/2023 02:18	1.6TB	2.0TB	1781027	pool-mensual-grande-prioritario
#####	mensual-job-zimbra	Full	132	backups-05-ece12d1.conicet.gov.ar-fd	22/6/2023 18:00	25/6/2023 03:52	1.7TB	2.8TB	15827587	pool-mensual-grande-prioritario
#####	mensual-job-sigeva-POSTULANTE	Full	165	backups-06-04c6ced33ec6.conicet.gov.ar-fc	22/6/2023 18:00	26/6/2023 21:16	6.1TB	6.8TB	10192379	pool-mensual-grande-prioritario
#####	mensual-job-sigeva-RESOLUCION	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	22/6/2023 18:01	22/6/2023 18:04	403.3MB	973.1MB	4927	pool-mensual-grande-prioritario
#####	mensual-job-sigeva-PROPIETARIO	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	22/6/2023 18:01	22/6/2023 20:08	35.6GB	42.2GB	211465	pool-mensual-grande-prioritario
#####	mensual-job-sigeva-PERSONA	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	22/6/2023 18:01	23/6/2023 17:07	592.2GB	677.4GB	2393103	pool-mensual-grande-prioritario
#####	mensual-job-sigeva-HANDLE	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	22/6/2023 18:00	22/6/2023 18:39	6.9GB	8.0GB	74830	pool-mensual-grande-prioritario
#####	mensual-job-sigeva-ARTICULO	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	22/6/2023 18:00	22/6/2023 18:05	1.0GB	1.1GB	2049	pool-mensual-grande-prioritario
#####	mensual-job-sigeva-LIBRO	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	22/6/2023 18:00	22/6/2023 18:01	2.3MB	2.4MB	3	pool-mensual-grande-prioritario
#####	mensual-job-sigeva-CONGRESO	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	22/6/2023 18:00	22/6/2023 18:01	29.2MB	30.6MB	33	pool-mensual-grande-prioritario
#####	mensual-job-sigeva-CAPITULO_LIBRO	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	22/6/2023 18:00	22/6/2023 18:01	6.1MB	6.4MB	9	pool-mensual-grande-prioritario
#####	mensual-job-wordpressconicet-multisitios	Full	10	apache-2_4-08-prod.gold.conicet.gov.ar-fd	22/6/2023 18:00	23/6/2023 03:54	208.8GB	222.8GB	1337428	pool-mensual-grande-prioritario
#####	mensual-job-glassfish-sigerh-jackrabbit	Full	165	backups-06-04c6ced33ec6.conicet.gov.ar-fc	22/6/2023 18:00	22/6/2023 22:27	105.3GB	111.8GB	4083583	pool-mensual-grande-prioritario
#####	job-repositorio-dspace-files	Full	132	backups-05-ece12d1.conicet.gov.ar-fd	22/6/2023 17:00	24/6/2023 05:57	1.6TB	1.8TB	2267050	pool-mensual-grande-prioritario
#####	job-tickets-02-prod.gold.conicet.gov.ar	Full	62	tickets-02-prod.gold.conicet.gov.ar-fd	22/6/2023 18:00	23/6/2023 06:50	247.0GB	316.1GB	5144263	pool-mensual-grande-prioritario
#####	mensual-job-glassfish-sigerh-documentoDigital-persona	Full	165	backups-06-04c6ced33ec6.conicet.gov.ar-fc	22/6/2023 18:00	22/6/2023 19:38	46.7GB	52.9GB	340151	pool-mensual-grande-prioritario
#####	mensual-job-glassfish-sigerh-documentoDigital-legajo	Full	165	backups-06-04c6ced33ec6.conicet.gov.ar-fc	22/6/2023 18:00	25/6/2023 00:13	3.1TB	3.5TB	223743	pool-mensual-grande-prioritario

pool-mensual-grande-prioritario: 000007L8, 000013L8



Name	Lev	Client	Client	Start time	End time	Size	Read byte	Files	Pool
mensual-job-atcat-8_5-03-prod.gold.conicet.gov.ar	Full	82	atcat-8_5-03-prod.gold.conicet.gov.ar-fd	26/6/2023 10:09	26/6/2023 10:10	482.7MB	723.6MB	4591	pool-mensual-miscelanea
mensual-job-atcat-9_0-03-prod.gold.conicet.gov.ar	Full	105	atcat-9_0-03-prod.gold.conicet.gov.ar-fd	26/6/2023 10:09	26/6/2023 11:12	25.4GB	70.3GB	934416	pool-mensual-miscelanea
mensual-job-atcat-9_0-02-prod.gold.conicet.gov.ar	Full	105	atcat-9_0-02-prod.gold.conicet.gov.ar-fd	26/6/2023 10:09	26/6/2023 10:09	121.6MB	138.0MB	1155	pool-mensual-miscelanea
mensual-job-atcat-9_0-01-prod.gold.conicet.gov.ar	Full	104	atcat-9_0-01-prod.gold.conicet.gov.ar-fd	26/6/2023 10:09	26/6/2023 10:10	778.8MB	2.0GB	34088	pool-mensual-miscelanea
mensual-job-atcat-8_5-08-prod.gold.conicet.gov.ar	Full	103	atcat-8_5-08-prod.gold.conicet.gov.ar-fd	26/6/2023 10:09	26/6/2023 10:10	249.7MB	448.8MB	2434	pool-mensual-miscelanea
mensual-job-atcat-8_5-09-prod.gold.conicet.gov.ar	Full	102	atcat-8_5-09-prod.gold.conicet.gov.ar-fd	26/6/2023 10:12	26/6/2023 10:16	1.8GB	5.8GB	5537	pool-mensual-miscelanea
mensual-job-dbs-mysql-sql-rabbit.rpc.conicet.gov.a	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	26/6/2023 10:21	26/6/2023 10:21	1.5MB	11.7MB	22	pool-mensual-miscelanea
mensual-job-dbs-mysql-web	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	26/6/2023 10:21	26/6/2023 10:24	852.1MB	5.7GB	63	pool-mensual-miscelanea
mensual-job-dbs-mysql-innovat-prod	Full	2	backups-02-dfa04be.gold.conicet.gov.ar-fd	26/6/2023 10:26	26/6/2023 10:31	2.1GB	12.0GB	25	pool-mensual-miscelanea
mensual-job-nginx-01-prod.gold.conicet.gov.ar	Full	93	nginx-01-prod.gold.conicet.gov.ar-fd	26/6/2023 10:32	26/6/2023 10:33	401.4MB	618.6MB	23669	pool-mensual-miscelanea
mensual-job-vcache-01-prod.gold.conicet.gov.ar	Full	92	vcache-01-prod.gold.conicet.gov.ar-fd	26/6/2023 10:09	26/6/2023 10:09	1.6kB	3.3kB	4	pool-mensual-miscelanea
mensual-job-haproxy-multisitio	Full	91	haproxy-principal-10-0-46-54-fd	26/6/2023 10:25	26/6/2023 10:25	47.1kB	181.2kB	18	pool-mensual-miscelanea
mensual-job-suitecrm	Full	90	suitecrm-01-prod.gold.conicet.gov.ar-fd	26/6/2023 10:25	26/6/2023 10:28	825.2MB	1.6GB	221358	pool-mensual-miscelanea
mensual-job-indico	Full	89	pgsql-9_6-02-prod.gold.conicet.gov.ar-fd	26/6/2023 10:09	26/6/2023 10:12	906.0MB	7.2GB	29144	pool-mensual-miscelanea

pool-mensual-miscelaneas-01: 000002L8

- ***Solapa 3: Cintas Externalizadas TODAS.xlsx***

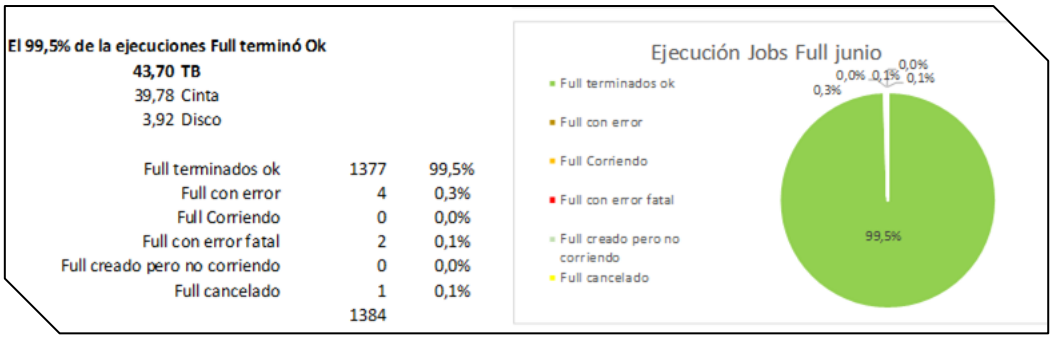
Corresponde al detalle de todas las cintas que se enviaron a Archivo. Tanto el reporte de la Solapa 2 y 3 se envían a Archivo con un remito para recepcionar el maletín estanco que contiene las cintas.

FECHA	POOL				
	Grande-Prioritarios	Miscelaneas-01	Prioritario	Complementarios	Hosting
jun-23	000007L8 - 000013L8	000002L8			

Traslado a Archivo: Estos listados junto con las cintas se trasladan al Archivo. Además, registran la entrada o salida mediante un remito. Según lo observado, las cintas se almacenan en una Caja Fuerte ignífuga:

Por otro lado, y cada mes, el área de Seguridad de la Información emite un reporte *"INFO_BKP-Jun23.pptx"* que contiene los siguientes datos acerca de los resguardos o Jobs ejecutados del mes, en este caso en junio: (*Resumen de ejecuciones, Ejecuciones totales del mes, Ejecuciones de los últimos meses, entre otros).*

Se adjunta extracto del informe, a modo de ejemplo:



Si bien el resultado de la verificación sobre el proceso de externalización fue satisfactoria, se observa la existencia de grupos de Jobs que no se encuentran debidamente documentados en el documento borrador *"Criterios de clasificación de los activos a resguardar.docx"* con lo cual no queda claro qué datos resguardan, su criticidad, tamaño y su frecuencia de traslado a sitio externo.

5.2.7 Registros y alertas por fallas en los procesos de resguardo (gestión de incidentes)

La GOS carece de un procedimiento formal de gestión de incidentes, ni otra documentación que se encuentre asociada a esta práctica. Asimismo, carece de una mesa de ayuda que centralice los pedidos, incidentes, consultas, entre otras cuestiones.

El organismo cuenta con una ticketera denominada "OTRS" *(Sistema de Mesa de Ayuda Configurable)* de código abierto, para llevar un registro y seguimiento de los incidentes producidos ante fallas en los procesos de resguardo y recuperación, entre otros incidentes.

Los incidentes son agrupados por colas, y cada cola corresponde a una categoría de incidente distinto y la gestiona un grupo de trabajo específico, a saber:

	Reportes remitidos OTRS (corresponde a cada cola de incidente)	Descripción	Total incidentes
1	***Reporte_Backup.xlsx***	Incidentes relacionados al proceso de resguardo.	245
2	Reporte_Identificacion.xlsx	Incidentes relacionados a la identificación de usuarios.	2936
3	Reporte_Mesa_de_ayuda.xlsx	Incidentes relacionados a la mesa de ayuda informática (aplicaciones ofimáticas, impresión, etc.)	2393
4	Reporte_Seguridad_de_la_informacion.xlsx	Denuncias y consultas varias.	81
5	Reporte_Seguridad_Informatica.xlsx	Pedidos de alta, baja y modificación de accesos.	484
6	Reporte_Soporte_Operaciones.xlsx	Incidentes relacionados a los servicios informáticos. (Subidas a producción de sistemas, pedidos de log, ejecución de scripts SQL, etc.)	1624

Según lo informado por el auditado:

> "*cada ticketera tiene un mail asociado, los usuarios escriben al mail y se genera el ticket automáticamente, y desde la mesa de ayuda que atiende esa ticketera contestan y gestionan a través de la herramienta. No hay una entrada única o mesa centralizada, los usuarios pueden escribir directamente a cada mesa, y en el caso de que la consulta no pertenezca a donde se recepcionó, se lo mueve a la ticketera correcta. Generalmente hay 4 ticketeras principales que reciben la mayoría de los tickets, Intranet (internos y externos), Sigeva (Internos y externos), Sigerh (solo personal del organismo), MesadeAyuda (soporte técnico).*"

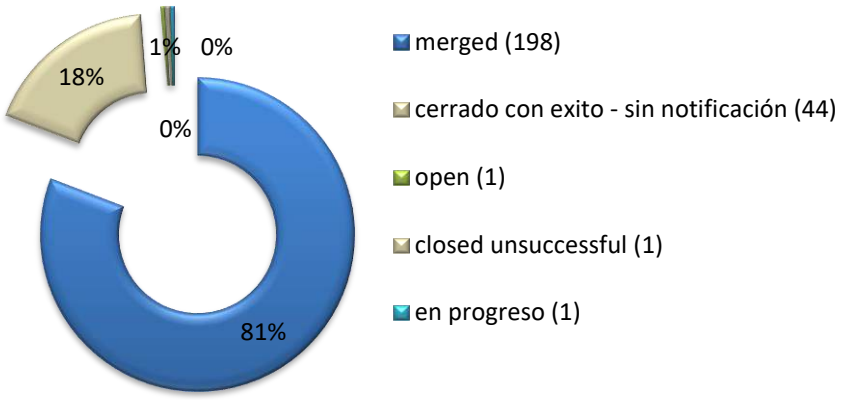
Respecto a la gestión de incidentes en relación al proceso de resguardo y recuperación, cabe destacar que BACULA genera de forma automática correos electrónicos ante la finalización, error o cancelación de un Job y en caso de detectarse un incidente, el sistema está configurado para generar un ticket directamente en OTRS para su derivación y resolución.

Desde el *"Reporte_Backup.xslx*", se pudo verificar que:

- **245** incidentes o tickets registrados forman el *universo de incidentes*, registrados desde marzo a junio de este año.

- OTRS maneja cinco estados, que se resumen en el gráfico siguiente con la cantidad de los incidentes/tickets, por estado:

Cantidad incidentes/tickets, según estado en OTRS



Entre los estados que puede tomar un ticket o incidente, se encuentra el estado "MERGED", del cual el auditado informa lo siguiente:

> *"El campo merged, en ocasiones se utiliza cuando un mismo evento afecta varios Jobs, como puede ser la cancelación de un grupo de Jobs por modificaciones o tareas sobre el equipo. En esos casos, el sistema de resguardo genera N alertas, 1 por cada Job, siendo fusionados todos los tickets en uno solo y figurando en el listado de Jobs con estado: merged. En el listado esos tickets no figuran con fecha de cerrado, porque la gestión queda asociado al ticket principal al que se fusiono".*

Para verificar la trazabilidad y la efectividad del proceso de resolución de incidentes en relación a la gestión de resguardo y recuperación, el auditado seleccionó un caso, en el cual menciona "*que adjunta una impresión de 1*

ticket completo con la evaluación de la causa, la gestión y la evidencia de resolución" mediante el documento *"Impresión ticket Backup.pdf*".

A continuación, se exponen los datos obtenidos de la lectura del documento arriba mencionado:

Fecha aviso	Job EN BACULA	Correo de BACULA / Ticket/incidente OTRS	Tipo Error
05.05.2023	18822	Correo Bacula informa error en la ejecución del Job 18822	"backups-02-dfa04be.gold.conicet.gov.ar-fd" 5.2.13 (19Jan13)
05.05.2023		2023050557001028 Ticket que Bacula genera automáticamente	Asunto: Bacula: Backup Error of backups-02-dfa04be.gold.conicet.gov.ar-fd Full
05.05.2023		-Área de Operaciones toma el ticket -Encuentra error	Error al realizar backup: eva_duplicado: Fri, 05 May 2023 07:31:44 -0300
06.05.2023	18848	Correo BACULA	"backups-02-dfa04be.gold.conicet.gov.ar-fd" 5.2.13 (19Jan13)
06.05.2023		Correo Bacula informa error en la ejecución del Job 18848	Asunto: Bacula: Backup Error of backups-02-dfa04be.gold.conicet.gov.ar-fd Full
06.05.2023		2023050657000223 Ticket que Bacula genera automáticamente	"backups-02-dfa04be.gold.conicet.gov.ar-fd" 5.2.13 (19Jan13)
08.05.2023		-Área de Operaciones toma el ticket -Encuentra error	Error al realizar backup: eva_duplicado: Fri, 05 May 2023 07:31:44 -0300
08.05.2023	18894	Correo Bacula informa error en la ejecución del Job 18894	"backups-02-dfa04be.gold.conicet.gov.ar-fd" 5.2.13 (19Jan13)
08.05.2023		-Área de Operaciones toma el ticket -Encuentra error	Asunto: Bacula: Backup Error of backups-02-dfa04be.gold.conicet.gov.ar-fd Full
08.05.2023		2023050857001586 Ticket que Bacula genera automáticamente	Asunto: Bacula: Backup Error of backups-02-dfa04be.gold.conicet.gov.ar-fd Full
10.05.2023	18986	Corre job, proceso OK	Client: "[2]backups-02-dfa04be.gold.conicet.gov.ar-fd"
Sin fecha		Captura de pantalla	Cerrado con éxito - sin notificación Fecha de creación 06/05/2023

No se pudo identificar ninguno de estos <u>números de ticket</u> en el "*Reporte_Backup.xlsx".*

No obstante, se decidió hacer la búsqueda a través de los campos "Titulo" y "Creado" ("*Backup Error of backups-02-dfa04be.gold.conicet.gov.ar-fd Full.",* que sería el campo clave, y por la fecha de creación "05/05/202"), siendo que tampoco se localizaron los tickets involucrados.

Adicionalmente, se procedió a la realizar la búsqueda con el auditado, a través de la herramienta OTRS donde tampoco se obtuvieron resultados positivos.

Por otro lado, se verifica que los incidentes/tickets de estado *merged*, carecen de fecha de cierre.

Adicionalmente, se efectuó un análisis sobre los campos que componen el "*Reporte_Backup.xslx"* extraído de la ticketera OTRS, el cual resulta que **muchos campos importantes no se encuentran configurados** como ser: *tiempos de respuesta del incidente, niveles de escalamiento, registro de solución,* entre otros.

Como resultado del análisis efectuado sobre el proceso, surgen las siguientes debilidades:

- **No existe documentación formal de la herramienta OTRS ni el detalle de cada campo.**

- La herramienta cuando un **incidente** tiene anexados otros incidentes (campo "**merged**"), **imposibilita conocer la fecha de cierre** de los mismos, debido a que el campo "Fecha de cierre" se encuentra vacío y la herramienta lo permite.

- OTRS **no tiene configurado campos importantes que resultan útiles** para registrar las tareas que se realizan para el tratamiento de un incidente.

- En la configuración actual de la OTRS, **no es posible efectuar la trazabilidad de los tickets asociados**.

- La herramienta **no permite detectar tiempos de respuestas y resolución de cada tickets.**

- **Se evidencia la existencia de campos útiles que no se encuentran utilizados en la herramienta.**

5.2.8 Realizar pruebas de recuperación

La *"Política de Resguardo y Recuperación De Información.pdf*" indica que las pruebas de recuperación se deben realizar periódicamente a intervalos no mayores a 6 (seis) meses.

Sin embargo, si bien manifiestan que se **realizan pruebas de recuperación**, las mismas **no son realizadas de forma programada y periódica**.

El auditado suministró el documento *"Impresión Ticket de Prueba de Restauracion.pdf"* como evidencia de la última prueba de recuperación realizada. **Las pruebas que se realizaron con anterioridad no se encuentran documentadas.**

Recomendación

Contemplar en el procedimiento en elaboración todos los aspectos y controles asociados a la generación de resguardos y recuperación (rotulación, reutilización, entre otros) asegurando que el mismo refleje la operatoria actual del proceso. Aprobar el procedimiento por la autoridad.

Documentar formalmente el criterio para clasificar los activos y/o utilizar una metodología aprobada, a modo de establecer la criticidad de los mismos y establecer prioridades al momento de definir su resguardo y recuperación.

Completar la información que contiene el inventario de servidores, indicando principalmente el entorno de procesamiento, qué herramienta se encuentran dando servicio, en qué ambiente y en qué CPD se aloja. Se sugiere evaluar la posibilidad de implementar una única herramienta que gestione tanto el inventario de hardware como las licencias de software.

Formalizar y documentar las pruebas de resguardo y recuperación de la información.

Documentar la configuración de todos los Jobs que se crean con toda su documentación respaldatoria (desde su creación hasta su fecha en producción), considerar que los mismos identifiquen fácilmente los activos de información a resguardar, como ser: formulario de resguardo, configuración de Jobs, datos del equipo de configuración, repositorio de pruebas, y Jobs, entre otros. Asimismo, asegurar que los números de Jobs sean datos claves y permitan efectuar una trazabilidad adecuada.

Consolidar los Jobs programados ya sea para resguardo y recuperación, y mantener el universo actualizado ante cada modificación

Considerar configurar en la herramienta BACULA, que los logs registren datos sensibles, como ser los usuarios que efectúan tareas en el proceso a modo de permitir efectuar trazabilidad.

Elaborar un procedimiento de monitoreo de incidentes que contemple todas las actividades necesarias para detectar en forma oportuna los desvíos referidos a la resolución de incidentes, y poder determinar a tiempo los eventuales incumplimientos por parte del proveedor.

Asimismo, asegurar la correcta trazabilidad de los incidentes, respecto a los procesos y sistemas relacionados (cambios a programas, requerimientos de accesos, inconvenientes en resguardos, entre otros).

Se sugiere analizar la conveniencia de contar con una mesa de ayuda o similar que centralice todos los incidentes/tickets.

Analizar la necesidad de configurar la herramienta de gestión de incidentes, a fin de asegurar independencia y confiabilidad a la hora de registrar, resolver y hacer monitoreo de los incidentes. De no ser posible, instrumentar mecanismos para disponer de controles por oposición al respecto. Configurar los campos de la herramienta a modo de evitar inconsistencias y/o entradas ambiguas y que los mismos permitan efectuar una adecuada trazabilidad.

Considerar la unificación de términos utilizados ya sea en la documentación como en las herramientas y sus reportes. Se sugiere buscar una solución posible para registrar la fecha de cierre de los incidentes relacionados con otros, o bien emplear otro mecanismo para tratar los incidentes similares a modo de buscar la causa de forma inmediata. Asimismo, asegurar que los números de tickets sean datos claves y se encuentren en los reportes de incidentes remitidos.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"El procedimiento MP-GOS-DGUyR-001 - del Resguardo/Backup a la Restauración contempla que las pruebas de recuperación sean programadas y ejecutadas periódicamente. Desde el momento de la implementación de la nueva infraestructura y modificación de los procedimientos. Por eso, al momento de la auditoría sólo se pudieron mostrar 2 ejecuciones con fechas 10/03/2023 y 17/7/2023.
La documentación de los Jobs de Backup está en la aplicación Bacula y en los archivos complementarios. La trazabilidad de los Jobs se realiza mediante el nombre del Job ya que es el dato que utiliza la herramienta Bacula. La herramienta Bacula se ejecuta en Linux y todas las acciones de los usuarios quedan registradas en bconsole y en logs del S.O. permitiendo la reconstrucción de las acciones de los usuarios en caso de requerirse."

Descripción del Curso de Acción a Seguir:
- Documentar formalmente el criterio para clasificar los activos.
- Completar la información que contiene el inventario de activos.
- Incorporar en el procedimiento de backup el versionado de los Jobs en Gitlab
- Asegurar una fácil trazabilidad de todos los elementos"

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: *"Responsable de Seg. Inf + Dirección de Ingeniería de Procesos + Dirección de Gestión de Usuarios y Red"*

Comentario final SIGEN

El comentario del auditado responde a lo observado en el punto. Se aclara que se pone foco en unificar los términos utilizados ya sea en la documentación como en las herramientas y sus reportes a modo de efectuar una adecuada y efectiva trazabilidad de los datos (incidentes, cambios en jobs, logs, jobs ejecutados, entre otros).

5.3 DETALLES SOBRE LA PRÁCTICA ACTUAL DE RECUPERACIÓN DE LA INFORMACIÓN

Si bien existe un "*Manual de Procesos MP-GOS-DGUyR-001 - del Resguardo/Backup a la Restauración.pdf*" borrador a nivel general, actualmente, **no existen procedimientos aprobados de recuperación de la información por sistema crítico y tal se mencionó en el punto 5.2.8 no se efectúan pruebas de recuperación en forma programada y periódica.**

A continuación, se detallan los pasos del procedimiento informal actualmente vigente, informado por el auditado:

5.3.1 Revisar solicitud de recuperación en la ticketera y aprobar o no la misma

El Responsable de Resguardo y Restauración tras recibir una solicitud de restauración de resguardo en la ticketera OTRS procede a validar con el Responsable del activo de información y el Responsable técnico del activo de información si se debe proceder con la solicitud de restauración.

Se registra en el ticket la autorización o rechazo de la solicitud.

- Si se autoriza la restauración, se procede con la localización de los medios de recupero.
- Si no se autoriza la restauración, se informa al Requirente y finaliza el proceso cerrando el ticket.

5.3.2 Localizar medios de recuperación

Una vez seleccionado el resguardo a recuperar, se ubica el medio de almacenamiento: en disco o en cinta (dentro del edificio o en el Archivo).

De requerirse un resguardo que se encuentra externalizado, se solicita al Responsable del Archivo del CONICET su ubicación y remisión a CONICET CENTRAL.

5.3.3 Ejecutar, validar y registrar ticket

El Responsable del Resguardo y Restauración registra en el ticket el resguardo y el medio que se recuperará:

➔ Recupera el resguardo en una ubicación alternativa, para no alterar los datos de producción.
➔ De producirse un error en la recuperación, que pueda ser resuelto por el Operador de Resguardo y Restauración, se trata de solucionar, de lo contrario se selecciona un medio de recuperación diferente junto al Responsable Técnico para realizar la recuperación desde otro medio.
➔ Copia la recuperación a la ubicación de intercambio.
➔ Da acceso al Requirente o al Responsable técnico a la ubicación de intercambio.
➔ Registra en el ticket el resguardo recuperado, el destino de la recuperación y su resultado.

Verificación de recuperación de un Job in situ

Durante la visita al CPD en CONICET Central, se realizó junto con el personal Responsable de la Seguridad de la Información una prueba de recuperación de uno de los últimos resguardos realizados.

El criterio de selección empleado para la selección del Job se basó en el tamaño del mismo, en vistas de poder ejecutar la restauración de manera completa durante el transcurso de la visita al CPD.

Durante la prueba se demostraron todos los pasos requeridos para completar un resguardo a través BACULA, de la interface “Bconsole” siendo estos:

1. La selección del tipo de recuperación,
2. El marcado de los archivos a recuperar.
3. La selección del servidor donde los archivos serán recuperados.
4. Confirmación del proceso dando lugar a la recuperación.

Las acciones efectuadas también se pueden ejecutar a través de la interfaz web Baculum, la cual actúa como “mascara” de Bconsole. Ambas interfaces son dos vías de acceso al BACULA. Para más información, remitirse al punto 4.3.1.

Por otro lado, el auditado remitió el reporte *“restores Auditoria.xlsx”* que detalla el registro de las 5 recuperaciones efectuadas en el mes de julio, se remarca la utilizada para la prueba.

JobId	Job	Name	Le
22804	RestoreFilesInLinuxWordpress.2023-07-03_10.57.09_43	RestoreFilesInLinuxWordpress	F
22999	RestoreFilesInLinuxGeneric.2023-07-06_09.45.29_27	RestoreFilesInLinuxGeneric	F
23002	RestoreFilesInLinuxPayara.2023-07-06_10.39.39_40	RestoreFilesInLinuxPayara	F
23005	Restore-dbsqlsrv01.conicet.gov.ar.2023-07-06_12.48.06_14	Restore-dbsqlsrv01.conicet.gov.ar	F
23129	RestoreFilesInLinuxPayara.2023-07-10_16.37.09_01	RestoreFilesInLinuxPayara	F

Por último, se verificó que los Jobs propios de recuperación que figuran en el extracto anterior, **no figuran en el universo de Jobs programados** provisto por el auditado *(JobsEnabled20230811.xlsx).*

Recomendación

Contemplar en el procedimiento de resguardo y recuperación en elaboración también los procedimientos formales de recuperación por sistema crítico. Aprobar los procedimientos por la autoridad.

Formalizar y documentar las pruebas de recuperación de la información. Establecer un esquema de pruebas anual y los mecanismos para efectuarlas.

Consolidar los Jobs programados ya sea para resguardo y recuperación, y mantener el universo actualizado ante cada modificación.

Rever el contrato con el proveedor UNITECH, incluyendo la cláusula de confidencialidad de los datos.

Incluir el tratamiento del sistema TRAMIX así como de sus datos, en los procedimientos de gestión de la tecnología informática del organismo, particularmente en los referidos a resguardo y recuperación de la información.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"El procedimiento "MP-GOS-DGUyR-001-del Resguardo/Backup a la Restauración" contempla los procedimientos de recuperación, para todo tipo de sistema.
Toda la documentación una vez pre-aprobada, sigue los procesos formales de aprobación.
Las pruebas de recuperación son contempladas en el procedimiento y están detallados los pasos, criterios y registros del proceso.
Todos los Jobs programados, ya sea para resguardo o recuperación, son consolidados y se mantienen actualizados en la herramienta Bacula.
El sistema tramix está incluido dentro de los activos cubierto por el procedimiento de Resguardo y Recuperación."

Descripción del Curso de Acción a Seguir:
- Aprobar los procedimientos de resguardo por la autoridad
- Formalizar y documentar las pruebas de recuperación de la información
- Establecer un esquema de pruebas anual y los mecanismos para efectuarlas.
- Rever el contrato con el proveedor UNITECH, incluyendo la cláusula de confidencialidad de los datos.

Fecha de Regularización Prevista: *"2do semestre 2024"*

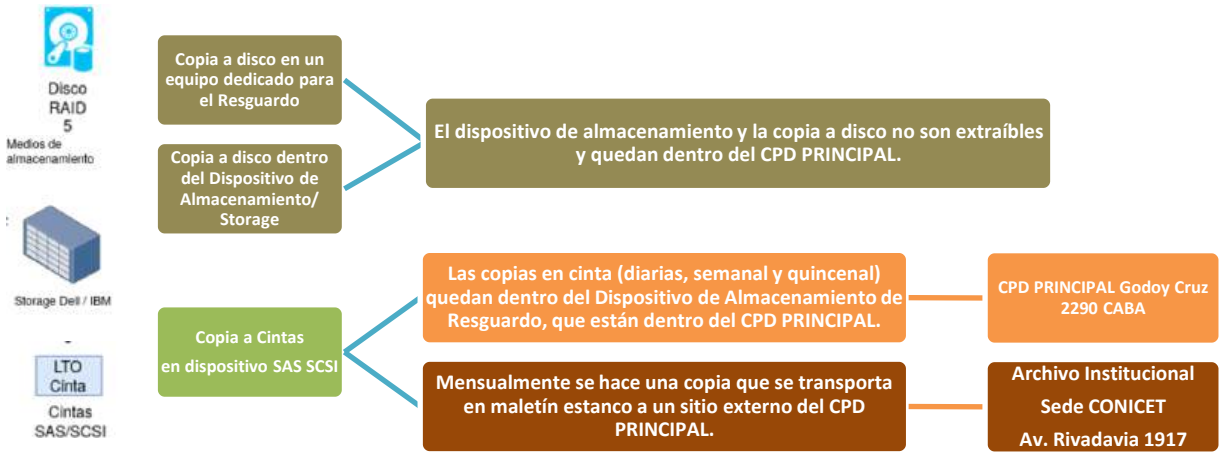
Área o Sector Responsable: *"Responsable de Seg. Inf + Dirección de Ingeniería de Procesos + Dirección de Gestión de Usuarios y Red."*

Comentario final SIGEN

El comentario del auditado responde parcialmente a lo observado en el punto. Se reitera lo recomendado en cuanto a documentar las prácticas habituales con el proveedor del sistema TRAMIX respecto a la gestión de resguardo y recuperación del mismo, así como también el registro de los Jobs utilizados.

5.4 SEGURIDAD FÍSICA DE LAS INFRAESTRUCTURAS CRÍTICAS

A continuación, se expone un gráfico que sintetiza la ubicación de los resguardos efectuados y los medios de almacenamiento utilizados:



Para verificar los accesos del personal al CPD Principal, se solicitó al auditado la siguiente información que, según nos fue informado, ha sido extraída del sistema de accesos del MinCyT.

- Último ingreso por agente:
  Se detectaron:
  - 4 usuarios que nunca han ingresado al CPD, y
  - 6 usuarios no han ingresado al CPD durante los últimos 12 meses.

Por lo anterior, se evidencia que **no se efectúa una revisión periódica mediante la cual se actualice/depure la lista de accesos permitidos.**

De la visita efectuada a la sede **Archivo**, surgen las siguientes debilidades:

- El Archivo es una oficina de la sede ubicada en Rivadavia 1917, la cual **no posee suficientes medidas de seguridad para alojar las cintas de resguardo.**

- Si bien el Archivo tiene instalados **aires acondicionados**, según lo informado por el auditado **uno de ellos presenta inconvenientes**.

Aire acondicionado fuera de servicio

- **La llave de la caja fuerte, donde se alojan los resguardos, se encuentra ensobrada y bajo guarda en un armario sin medidas de seguridad**

- **No se cuenta con un armario ignífugo para el almacenamiento de cintas.**

- **El Archivo presenta material combustible a lo largo de todas las salas aledañas a la caja fuerte.**

Para más información, remitirse al punto 4.2 y 4.3.3.

Recomendación

Para CPD Principal:

Efectuar revisiones periódicas del personal autorizado a ingresar al CPD y los registros de accesos efectuados.

Para el Archivo:

Se sugiere evaluar la posibilidad proveer de mejores condiciones de seguridad a la zona donde se aloja la caja ignifuga que contiene las cintas.

Es fundamental disponer de controles preventivos como, por ejemplo, control de acceso biométrico, registro de visitas, sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de resguardo y los registros no electrónicos críticos, etc.

Se sugiere implementar un mecanismo de control que asegure la protección y resguardo de la llave de la caja fuerte de las cintas a personal no autorizado.

Los materiales peligrosos o combustibles deben ser almacenados a una distancia segura para evitar el daño de un desastre que afecte al CPD.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"Sin comentarios"

Descripción del Curso de Acción a Seguir:
"- Evaluar la posibilidad de proveer de mejores condiciones de seguridad a la zona donde se aloja la caja ignífuga que contiene las cintas, dentro de las posibilidades presupuestarias del Organismo.
- Mejorar las condiciones de resguardo de la llave de la caja fuerte.

- Se verificará de manera periódica que la lista de personas autorizadas a ingresar al CPD Principal se encuentre actualizada."

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: *"GOS - DGUR - DIP"*

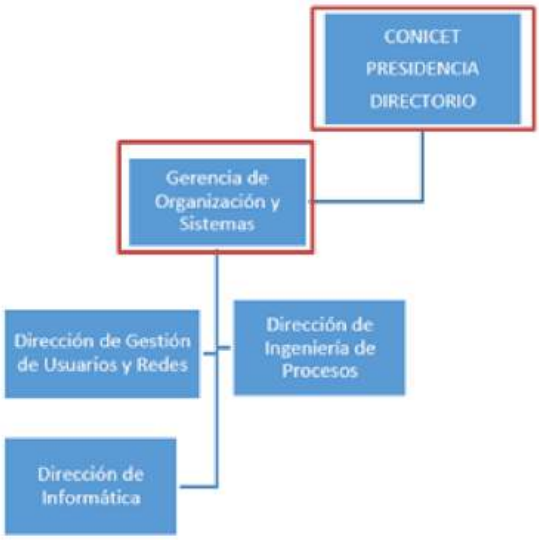
Comentario final SIGEN

Lo mencionado en la respuesta del auditado se encuentra alineado a las recomendaciones de SIGEN.

5.5 ORGANIZACIÓN INFORMÁTICA

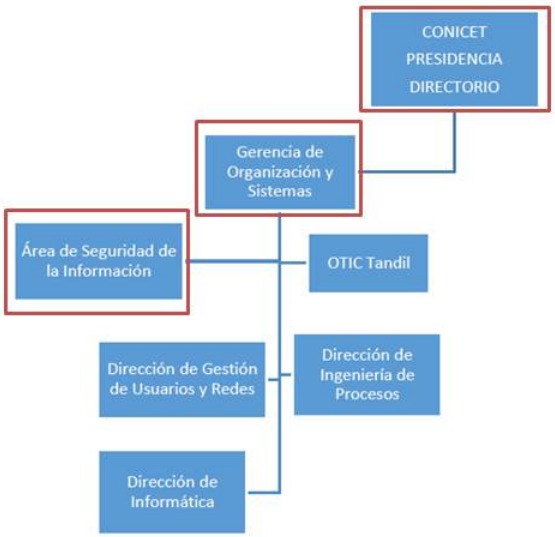
La Gerencia de Organización y Sistemas (en adelante, GOS) depende de la máxima autoridad del Organismo.

Según el documento remitido por el auditado *"Organigrama_Roles_Funciones_final.pdf"*, el último organigrama del organismo (estructura organizativa de primer y segundo nivel operativo) ha sido aprobado mediante el Decreto N° 310/2007. Asimismo, el mencionado decreto aprueba las responsabilidades, funciones y acciones correspondientes a las direcciones que dependían de la GOS, en aquel momento.



Asimismo en el mismo documento se adjunta el organigrama actual de la GOS, que **a la fecha carece de su aprobación formal**, y es el siguiente:

Organigrama Actual de la Gerencia de Organización y Sistemas



Como se visualiza, **el área de Seguridad de la Información depende de la GOS** y ésta depende de la máxima autoridad del organismo.

En la siguiente tabla se expone la dotación de la GOS actual, en cuanto al personal de sistemas (*técnico y administrativo*):

	Cant. de agentes
Gerencia de Organización y Sistemas (GOS)	5
• **Dirección de Gestión de Usuarios y Redes**	23
• **Dirección de Ingeniería de Procesos**	14
• **Dirección de Informática**	23
• **Área de Seguridad de la Información**	4
• **OTIC Tandil**	19
TOTAL	**88**

A su vez, en el mencionado decreto se incluyen los roles y funciones de las áreas de la GOS, salvo las áreas “Seguridad de la Información” y la “Oficina de Tecnología de Información y Comunicaciones (OTIC Tandil[4]) que fueron creadas posteriormente.

De la lectura sobre los roles y funciones, no se identificó qué áreas se encuentran involucradas en la gestión de resguardo y recuperación ni sus tareas relacionadas.

Por su parte, el auditado informó lo siguiente:

[4] RESOL-2021-656-APN-DIR#CONICET (26 de Marzo de 2021) crea la Oficina de Tecnología de Información y Comunicaciones (OTIC) de Tandil dependiente de la Gerencia de Organización y Sistemas (GOS) cuya misión es la de colaborar en el sostenimiento de los servicios que ésta brinda.

- Seguridad Informática "*Con respecto a esta Área, si bien no aparece en el organigrama del 2007, las funciones que le corresponden se encontraban atomizadas en la Dirección de Gestión de Usuarios y Redes y en la Dirección de Informática. Durante los últimos años, fue necesaria la constitución de un Área específica para dar respuesta a los crecientes y particulares desafíos que se enfrentan en términos de Seguridad:*

- OTIC Tandil: "…*Finalmente, en marzo de 2021 mediante la Resolución RESOL-2021-656-APN-DIR#CONICET se formaliza la creación de la Oficina de Tecnología de Información y Comunicaciones (OTIC) de Tandil dependiente de la Gerencia de Organización y Sistemas (GOS) cuya misión es la de colaborar en el sostenimiento de los servicios que esta brinda, tal como se establece en el Artículo 1".*

Según la RESOL-2019-2622-APN-DIR#CONICET de diciembre 2022 en su Artículo 3° designó los integrantes del Comité de Seguridad de la Información y al Responsable de Seguridad de la Información.

Conviene acotar que dentro de la GOS, existe el área "Mesa de Entrada", que depende de la Dirección de Gestión de Usuarios y Red y las áreas "Archivo" y Repositorio Institucional" que dependen de la Dirección de Ingeniería de Procesos. Áreas que no efectúan tareas propias a la tecnología de información.

Recomendación

Obtener la aprobación formal de la nueva estructura de la Gerencia de Organización y Sistemas de modo que represente las dependencias actuales, asegurando que queden claras las responsabilidades.

Asimismo, consolidar en un solo documento las misiones y funciones de cada área de la Gerencia de Organización y Sistemas, en línea con la estructura que se apruebe, considerando que cada puesto de trabajo cuente con las definiciones de misiones y funciones, dependencias funcionales y asignación de responsabilidades. Asimismo, notificar formalmente al personal de sus deberes y responsabilidades.

En la misma línea, incorporar en el documento de misiones y funciones las tareas de resguardo y recuperación a las áreas con injerencia en esta operatoria.

Asignar las responsabilidades por la Seguridad de la Información a un área independiente de la unidad de TI, constituyendo de ese modo, un mecanismo de control por oposición.

Tal como se indica en las Normas de Control Interno para Tecnología de la Información –Res. N° 87/22- en cuanto a que *"en aquellas organizaciones que manejen importantes volúmenes monetarios y/o gestionen información o infraestructuras de alta criticidad para el Estado Nacional, deberán asignarse las responsabilidades por la Seguridad de la Información a un área independiente de la unidad de TI, constituyendo de ese modo, un mecanismo*

de control por oposición", se insta a considerar asignar las responsabilidades por la Seguridad de la Información a un área independiente de la unidad de TI.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"Tal como se menciona en el documento remitido, el camino de adecuación de la organización de la GOS está en marcha. Se encuentra en proceso de aprobación formal la nueva estructura de la GOS.
Con respecto a las responsabilidades por la Seguridad de la Información, como se mencionara oportunamente la misma depende de la GOS, teniendo independencia de las áreas responsables de TI."

Descripción del Curso de Acción a Seguir:
"Ya existe un proyecto de adecuación de la estructura que se encuentra en vías de aprobación. Una vez que sea aprobado, se presentará en reunión de Directorio del CONICET la propuesta para formalizar el área de Seguridad de la Información dentro de la GOS, dependiendo directamente de la Gerencia y con independencia de las áreas específicas de IT."

Fecha de Regularización Prevista: *"2 do semestre 2024"*

Área o Sector Responsable: "*Gerencia de Organización y Sistemas"*

Comentario final SIGEN

Lo mencionado en la respuesta del auditado se encuentra alineado a las recomendaciones de SIGEN.

No obstante, se insta a considerar asignar las responsabilidades por la Seguridad de la Información a un área independiente de la unidad de TI, que dependa de la máxima autoridad.

5.6 PLAN INFORMÁTICO ESTRATÉGICO

El CONICET ha remitido la primera versión del "*Plan estratégico de TI 2023 – 2025.pdf*", que el Directorio aprobó formalmente el 7 de junio del corriente durante la labor de esta auditoría mediante el ME-2023-66390524-APN-CONICET#MCT (IF-2023-61016382-APN-GOYS#CONICET).

De la lectura del mismo surge que:

- El plan no detalla las actividades a llevar a cabo para el cumplimiento de cada uno de los proyectos, fechas estimadas de cumplimiento, designación de responsables y recursos asignados, costos, entre otros aspectos.

- Por otro lado, dentro del mismo documento se incluye el plan operativo anual de este año, que menciona, entre otras, las actividades y productos finales siguientes:

ACTIVIDADES	PRODUCTOS FINALES
Continuar con la implementación de la política de seguridad de la información contemplando las necesidades de la Red Institucional	Políticas de Seguridad del CONICET aprobada y comunicada
Elaborar y formalizar un programa de implementación de Tecnologías de la Información y Comunicación (TIC) y su correspondiente plan operativo	Plan Estratégico de TI elaborado

Cabe hacer mención que estas **actividades carecen del detalle de las tareas asociadas a cada uno de estos dos proyectos, los responsables, los plazos, los beneficios a obtener así como sus costos asociados.**

El plan incluye un gráfico con los sistemas que desarrolla y gestiona la GOS, **sin embargo los sistemas difieren de la lista de sistemas remitida por el auditado en la planilla completada a solicitud de esta auditoría.**

No se obtuvo evidencia acerca de la revisión sistemática que asegure la actualización permanente del plan informático y plan operativo anual a efectos de ajustar posibles desvíos, ni documentación de seguimiento de avances por proyectos.

Según lo informado por el auditado, en cuanto al seguimiento de avance de los proyectos, la GOS utiliza la plataforma para gestión y trabajo en equipo denominada JIRA.

Si bien utilizan la herramienta antes mencionada, **no cuentan con metodologías o procedimientos formales destinados a regular la gestión de proyectos**.

Recomendación

Incorporar al plan, según corresponda al plan estratégico o plan operativo, los aspectos que reflejen los proyectos y tareas relacionados con la tecnología informática (software de base, aplicativos, hardware, capacitación, etc.

Lo anterior permitirá:

- Contribuir a asegurar el alineamiento de las actividades en marcha con los objetivos planteados en las políticas públicas dispuestas en materia informática,
- Generar herramientas para permitir el adecuado seguimiento del cumplimiento del plan y la oportuna detección de desvíos,
- Asegurar el necesario apoyo para la ejecución de las actividades planificadas y la asignación de recursos, entre otros.
- Formalizar los objetivos y metas correspondientes a la tecnología informática.

Dicho Plan debe estar alineado con los objetivos estratégicos y el presupuesto del organismo y debe considerar los aspectos mencionados en el punto 2 de la Norma Res. N° 87/2022 SIGEN referido al "Plan estratégico de TI".

Consolidar toda documentación referente a la planificación y seguimiento de los proyectos informáticos, incluyendo el sistema bajo análisis. Asegurar que la herramienta pueda ser provechosa a la hora de planificar y registrar el seguimiento de los proyectos planificados.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"Para que la dirección de la organización pueda realizar el seguimiento correspondiente se considera la herramienta del Plan Anual Operativo (POA) como el instrumento adecuado y vigente, siguiendo el punto 2.6 de las Normas de Control Interno para Tecnologías de la Información - Sector Público Nacional y otras recomendaciones de la SIGEN.
Siendo el Plan Estratégico de TI (PETI) un plan plurianual que contiene el detalle de los proyectos, para luego alinearse año a año con el POA del Organismo. En caso que la dirección lo considere, se realizaría la actualización del PETI."

Descripción del Curso de Acción a Seguir:
"Incorporar al POA 2024 los aspectos que reflejen los proyectos, tareas y responsables relacionados con la tecnología informática, alineado con el PETI.
Consolidar el seguimiento de los proyectos informáticos, reflejándolo en el POA."

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: *"Gerencia de Organización y Sistemas"*

Comentario final SIGEN

El curso de acción a seguir indicado por el auditado, se encuentra alineado a las recomendaciones de SIGEN. No surgen comentarios adicionales.

5.7 POLÍTICAS Y PROCEDIMIENTOS

La Política de Seguridad de la Información de CONICET fue aprobada mediante la RESOL-2022-2296-APN-DIR#CONICET del 27 de diciembre de 2022. La misma incluye la aprobación del Comité de Seguridad de la Información y la designación del Responsable de Seguridad de la Información de ese Comité.

La política está adecuada a la DA 641/2021 *"Requisitos mínimos de Seguridad de la Información para Organismos".*

El auditado remitió el documento creado en 2020, "*Buenas-practicas-básicas-para-contraseña.pdf*", que define las "buenas prácticas para la creación de contraseñas", sin embargo **no forma parte de las políticas y procedimientos de la gestión de acceso, se trata de una guía.**

Cabe hacer mención que el ***Plan estratégico de TI 2023 – 2025.pdf*** remitido, contempla un proyecto que consiste en *"Administrar y actualizar los manuales de procedimientos y políticas de la TI"*.

No obstante, el CONICET carece de los siguientes procedimientos:

- Administración de proyectos informáticos.
- Administración de usuarios (altas, bajas y modificación de usuarios)
- Adquisición de software y hardware
- Atención de la mesa de ayuda/servicios informáticos
- Gestión de cambios a los programas
- Gestión de incidentes
- Gestión de licencias de software
- Gestión de vulnerabilidades
- Implementación y revisión de registros de transacciones o logs
- Metodología de administración web
- Propiedad y clasificación de la información
- Seguridad física del centro de cómputos

Recomendación

Será de suma relevancia la implementación de lo definido en la Política de Seguridad atento a la sensibilidad de los datos que administra el CONICET. Se sugiere revisar los lineamientos de la misma, para asegurar que todos los ítems en relación a la gestión de resguardo y recuperación se encuentren contemplados, como ser rotulación de cintas y reutilización de medios de almacenamiento.

Adicionalmente, desarrollar e implementar los procedimientos faltantes y para los procedimientos existentes, documentar la evidencia de su aprobación e indicar sus fechas de vigencia.

Se deberá involucrar a la Unidad de Auditoría Interna en el circuito de aprobación de los procedimientos en relación a la gestión informática conforme lo establece la Resolución Nº 162/2014 SIGEN.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"El procedimiento de Resguardo y Restauración contempla la rotulación de los medios.
La reutilización de los medios está planteada en el documento "Criterios de clasificación de los activos a resguardar" e implementado en la programación de los Jobs.
El documento será adecuado en base a las recomendaciones."

Descripción del Curso de Acción a Seguir:
- Adecuar el documento "Criterios de clasificación de los activos a resguardar" en base a las recomendaciones.
- Continuar con la formalización de procedimientos faltantes.

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: *"Responsable de Seg. Inf + Dirección de Ingeniería de Procesos + Dirección de Gestión de Usuarios y Red."*

Comentario final SIGEN

El curso de acción a seguir indicado por el auditado, se encuentra alineado a las recomendaciones de SIGEN. Si bien el procedimiento incluye ciertos aspectos sobre el formato del rótulo de la cinta, se reitera que corresponde adicionar el circuito empleado de rotulación de los medios de almacenamiento, o bien hacer referencia al documento formal que detalle esta práctica.

5.8 GESTIÓN DE CAMBIOS/CONFIGURACIÓN DE LOS JOBS

El organismo **no posee un procedimiento formal de gestión de cambios (programas aplicativos, Jobs/scripts, configuraciones)**,

Si bien en el procedimiento borrador "*Manual de Procesos MP-GOS-DGUyR-001 - del Resguardo/Backup a la Restauración.pdf*", se contemplan las responsabilidades y algunos pasos del proceso, el mismo resulta incompleto dado que no incluye el circuito completo desde su solicitud hasta su implementación en producción.

Según lo informado por el auditado, para poder conservar todo lo relacionado a la implementación, configuración y Jobs asociados se mantiene un

repositorio llamado “BACULA” en la herramienta de control de versiones GitLab oficial de CONICET. Sin embargo, **esta práctica no se encuentra formalmente documentada**

Para el desarrollo de software, utilizan la herramienta JIRA, de la cual no se obtuvo el reporte de cambios o proyectos registrados a la fecha, solo algunas capturas de pantallas a modo de ejemplo.

Cabe agregar que no existe documentación formal que concentre detalles de los Jobs creados en BACULA: nombre del Job, id, qué datos resguarda, en qué medio de almacenamiento, frecuencia de ejecución, criticidad, prioridad, solicitantes, autorizantes y responsables de su implementación, entre otras cuestiones.

Por la lectura de los documentos asociados al EX-2022-118090051-APN-GA#CONICET que refiere a la contratación del proveedor UNITECH, amerita mencionar algunas particularidades, debido a que se trata de un sistema considerado “critico”:

- **La base de datos es soportada y mantenida por UNITECH junto con personal de la GOS del Organismo.**
- **En el contrato no existe una clausula puntual referida a la confidencialidad de la información.**
- **Se adiciona que las prácticas habituales con el proveedor no se encuentran documentadas formalmente, como por ejemplo como se recupera un resguardo en la nube AWS, en la cual interviene el proveedor y de la cual no se cuenta con información, salvo que el AWS – VMware pertenecería al Organismo.**

Recomendación

Desarrollar un procedimiento de Cambios a Programas formal alineado a lo establecido en las Normas de Control Interno para Tecnología Informática dispuestas por SIGEN, mediante la Res. N° 87/2022, punto 7 *“Desarrollo, mantenimiento o adquisición de software de aplicación”.*

El procedimiento de cambios debe incluir el circuito tanto para cambios efectuados por personal interno como para los de un tercero.

Prever cláusulas de confidencialidad de la información en las futuras contrataciones.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"Sin comentarios."

Descripción del Curso de Acción a Seguir:
- Desarrollar un procedimiento de Cambios a Programas formal alineado a lo establecido en las Normas de Control Interno para Tecnología Informática dispuestas por SIGEN, mediante la Res. N° 87/2022, punto 7 "Desarrollo, mantenimiento o adquisición de software de aplicación".
- El procedimiento de cambios debe incluir el circuito tanto para cambios efectuados por personal interno como para los de un tercero.
- Prever cláusulas de confidencialidad de la información en las futuras contrataciones.

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: *"Responsable de Seg. Inf + Dirección de Ingeniería de Procesos + Dirección de Gestión de Usuarios y Red"*

Comentario final SIGEN

El comentario del auditado responde a lo observado en el punto. No se efectúan comentarios adicionales.

5.9 GESTIÓN DE USUARIOS

El auditado **no cuenta con un procedimiento formalmente aprobado** para la gestión de alta, baja y modificación de los usuarios.

Según lo informado en el documento **borrador** *"Intranet de CONICET.docx",* el organismo administra la autenticación de usuarios mediante la Intranet de CONICET, sobre Apereo CAS 6.6, (protocolos CAS, SAML 2.0, OpenID, entre otros).

Particularmente para la administración de permisos de accesos, el organismo cuenta con una aplicación específica desde la cual los responsables de Seguridad de la Información administran de manera centralizada los permisos a todas las aplicaciones de la intranet.

Resultado de análisis de permisos de usuarios al sistema BACULA y su entorno de procesamiento:

Usuarios con permisos al sistema BACULA:

Respecto a los permisos de accesos al software utilizado para la gestión de resguardo y recuperación, el auditado proporcionó el documento *"Baculum - BACULA Web Interface – Usuarios.xlsx"*, que consta de 9 usuarios.

	Username	Descripti on	Roles	Área a la cual pertenece
1	admin83187b05	-	admin	Esta cuenta se generó y utilizó durante la instalación del sistema.
2	operator-jc-3c508328	-	admin	Operaciones

3	**cmiano-e7b2ebb3**	Acceso de visor	funcional-view	Dirección de Gestión de Usuarios y Red
4	**cristinag-1baa46dd**	-	funcional-view	Seguridad de la Información
5	**jdorado-d321d23a**	-	funcional-view	Responsable de la Seguridad de la Información
6	**jp-92972ef0f6**	JuanS	funcional-view	Director de Gestión de Usuarios y Red
7	operator-a0601022	**-**	**funcional-view**	**Operaciones**
8	**placasse-f3e64244f4**	-	funcional-view	Seguridad de la Información
9	**pdimuzio-c9c5d0ed**	-	only-view	Dirección de Gestión de Usuarios y Red

Según lo informado, en BACULA:

- La cuenta "*admin83187b05*" se encontraría deshabilitada, condición que **no pudo ser verificada debido a la carencia del extracto de usuarios** desde el sistema correspondiente.

- Existencia de una cuenta genérica "*operator-a0601022*", la cual se desconoce el agente que la utiliza.

Por su parte, el auditado no ha remitido los **extractos del detalle de los usuarios con permiso** de acceso tanto al servidor Linux (donde reside el Bacula) como a la base de datos utilizada por Bacula, sin embargo informó lo siguiente:

Usuarios con permisos al Servidor Linux

La extracción de usuarios linux donde reside bacula:

operator-21d9ce59: R...

operator-jc-3c508328: J...

- Ambas cuentas pertenecen a agentes de "Operaciones"-

Usuarios con permisos a la Base de datos BACULA

Según lo informado por el auditado, *"el usuario con máximos privilegios en la DB es bacula-db-cbcd1fe632: Agente de Operaciones"*

el usuario con máximos privilegios en la DB es bacula-db-cbcd1fe632: J...

- 1 cuenta de usuario del área de Operaciones (*operator-jc-3c508328*) contarían con permisos de máximos privilegios en el servidor Linux, en la base de datos del BACULA y en el sistema BACULA en sí. **Esto no ha podido ser verificado debido a la carencia de los extractos de usuarios correspondiente.**

Por otro lado, si bien el auditado remitió el documento *"MP-GOS-DGUyR-003 - de la solicitud a la gestión y baja de permisos de aplicaciones.pdf",* el mismo carece de la aprobación formal por parte de la autoridad.

Por lo relevado, **no se realizan revisiones periódicas de usuarios y perfiles de usuarios.**

Recomendación

Desarrollar un procedimiento de gestión de usuarios (incluyendo el tratamiento de usuarios críticos o de emergencia), que incluya los pasos a seguir ante un alta, baja o modificación de usuario. Obtener las aprobaciones de la autoridad.

Designar responsables tanto para la revisión periódica de perfiles de usuarios, como también para el monitoreo periódico de la actividad de los mismos.

Asegurarse la existencia de documentación formal sobre la estructura de roles y permisos, teniendo en cuenta todos los perfiles creados para la gestión de los sistemas críticos.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"En la auditoría se proveyó el procedimiento "MP-GOS-DGUyR-003- de la solicitud a la gestión y baja de permisos de aplicaciones.pdf", el cual contempla las Altas, Bajas y Modificaciones de permisos, como también la revisión y remoción periódica de los permisos, asignando la responsabilidad de la ejecución al Departamento de Seguridad Informática. El mismo se encuentra en proceso de aprobación.
La revisión y remoción de permisos se hace mensualmente, también se mostró evidencia de la ejecución en la auditoría. (Tickets mensuales de bajas, en la ticketera de Seguridad-Informática)
Las credenciales de acceso a los recursos de infraestructura son administradas por la DGUyR, quien se encuentra actualizando los sistemas de autenticación y autorización."

Descripción del Curso de Acción a Seguir:
"- Una vez finalizada la actualización del sistema de autenticación, Desarrollar un procedimiento de gestión de usuarios (incluyendo el tratamiento de usuarios críticos o de emergencia), que incluya los pasos a seguir ante un alta, baja o modificación de usuario de los recursos de infraestructura."

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: "*Dirección de Ingeniería de Procesos + Dirección de Gestión de Usuarios y Red*

Comentario final SIGEN

Los cursos de acción a seguir mencionados por el auditado se encuentran alineados a la recomendación de SIGEN. Cabe aclarar que las observaciones

surgieron de la documentación remitida y del relevamiento efectuado durante la auditoría. El documento remitido *"MP-GOS-DGUyR-003- de la solicitud a la gestión y baja de permisos de aplicaciones.pdf"* no especifica el circuito de administración de usuarios ni el tratamiento de usuarios especiales ni de emergencia.

5.10 PLAN DE CONTINGENCIA

El auditado proporcionó el documento *"Plan de Contingencia Informático.pdf" (en adelante, PCI).* Dada la reciente creación del mismo (primera versión, 15 de abril del corriente), el auditado ha informado que el PCI **se encuentra en revisión y pendiente de aprobación por parte de la máxima autoridad**.

De la lectura del PCI surgen los siguientes aspectos a remarcar:

"SERVICIOS CRÍTICOS Y ORDEN DE RESTAURACIÓN
Sistemas críticos: "Se definen como Sistemas y Servicios críticos para el CONICET los siguientes:

LISTA DE SISTEMAS CRÍTICOS
1. Tramix Liquidación de haberes
2. Intranet
3. SIGERH
4. SIGEVA
5. SIAF
6. Página web
7. Resto de sistemas

LISTA DE SERVICIOS CRÍTICOS
- *Servicio eléctrico*
- *Enlaces de Comunicaciones*
- *Servicio de VDI (Servicio de Virtualización de Escritorios)*
- *Servicio de Correo Electrónico*
- *Servicio de Respaldos*
- *Servicio de impresión y archivos*
- *Otros servicios"*

SITIOS ALTERNATIVOS:
***"1.** Servicio en la Nube de AWS, para la ejecución del sistema Tramix liquidación de Haberes, y otros sistemas críticos.*
***2.** Sitio alternativo de respaldo de información, Sede Conicet Av. Rivadavia 1917.*
Dependiendo de la gravedad de la contingencia, se analizará la posibilidad de contratar un sitio alternativo."

Por lo expuesto precedente y el relevamiento llevado a cabo, surgen las siguientes debilidades:

- En el documento completado y enviado a esta auditoría por parte del auditado, *"Detalle de todos los sistemas que posee el CONICET.xls"*, **no figuran otros sistemas catalogados como "críticos",** pudiéndose entender que entrarían en la categoría "*7. Resto de sistemas":*

  - BICYT - Buscador Integral de Ciencia y Tecnología
  - CRM - CRM de la Gerencia de Vinculación Tecnológica
  - Datawarehouse
  - DSpace
  - ELEC - Elección
  - INTWEB - Correo
  - IUI - Identificación Usuario Intranet
  - OTRS - Ticketera
  - PGD - Sistema de Planes de Gestión de Datos
  - Portal Multisitio
  - RI - Repositorio Institucional

- SIBI - Sistema informático de bienes inventariables
- SIGEF - Sistema Integral de Gestión de Fondos
- SIGEO - Sistema Integral de Gestión de Organizaciones
- SINE - Sistema Integral de Notificaciones Electrónicas
- SVT - Sistema de Vinculación y Convenios.

- **Respecto al servicio en la nube de AWS, no queda claro qué sistemas además del TRAMIX, harán uso de ese servicio en caso de contingencia.**

- **El sitio alternativo en la Sede del Archivo de Rivadavia 1917, actualmente no está implementado ni acondicionado como tal.**

- **El desarrollo del PCI está en proceso, y aún carece de definiciones concretas:**

    - No figura claramente la prioridad de recuperación de cada sistema crítico.
    - Bajo “Servicios Críticos y Orden de Restauración” del PCI, como último punto figura *“7. Resto de los sistemas”,* no dejando claro cuáles son todos los restantes sistemas del organismo que tienen que ser recuperados, dado que al estar bajo este título se entiende que son considerados también críticos, y por lo tanto, restaurados en contingencia.
    - No detalla en qué sitio alternativo se efectuará la recuperación de cada sistema/servicio crítico.
    - En cuanto a la estructura del Plan, si bien cuenta con cierta información, no detalla de manera suficiente: responsabilidades, Acuerdo de Niveles de Servicio (SLA), formularios involucrados, contactos, y los pasos a seguir desde la declaración de una contingencia hasta la restauración y vuelta a la operatoria normal, a saber:
        - No se contempla la evaluación del daño.
        - No se mencionan los tiempos de recuperación y objetivos de recuperación por sistema crítico.
        - No incluye procedimiento de restauración por parte de terceros ni SLA con proveedores asociados (TRAMIX).
        - No se cuenta con los procedimientos técnicos para restaurar cada uno de los sistemas críticos.
        - No especifica la gestión de comunicaciones con los datos de contacto, esquemas de guardias, entre otros aspectos.
        - No incluye lineamientos ni diagramas de pruebas y mantenimiento del plan.
        - El apoyo a los usuarios y concientización no se encuentra considerado en el mismo.
- El PCI no hace referencia a estos aspectos claves de control: clasificación de activos, seguridad física de los CPD, procedimientos de gestión de resguardo, incidentes, política de seguridad, inventario de software y hardware, contactos de emergencia, gestión de comunicaciones, entre otros.

Cabe hacer mención que en el "*Plan estratégico de TI 2023 – 2025.pdf*" remitido, surge un proyecto que consiste en implementar sitios alternativos externos de contingencia a los servicios críticos. **Sin embargo no se obtuvo documentación respaldatoria formal al respecto.**

Es dable hacer mención que, tal como se deja constancia en otros puntos de este informe, el organismo carece de determinados procedimientos asociados a la implementación y puesta en marcha del PCI, como ser el referido a la gestión de incidentes y mesa de ayuda, el cual indicaría los pasos a seguir en caso de requerir escalar un incidente a contingencia, así como el de resguardo y recuperación de la información.

En el documento remitido *"Respuesta sobre Plan de Continuidad.docx",* el auditado adjunta la prueba realizada sobre una recuperación en ambiente de contingencia correspondiente al sistema TRAMIX, tomado a modo de ejemplo, y detalla lo siguiente:

"Conicet efectuá una subida mensual de la Base de Datos Oracle del sistema de liquidación de Haberes al ambiente en la nube de AWS.
- Semestralmente se solicita al proveedor de la aplicación una restauración de la última base subida en el ambiente del sitio de contingencia, AWS. Última actualización 09/02/2023. Queda registrado en el Sistema de Tickets del proveedor y en el informe mensual que envía el proveedor.
- Semestralmente se realiza una prueba de restauración utilizando los medios externalizados. Última prueba 10/03/2023. Queda registrado en el sistema de Tickets del organismo."

Se verificó que lo remitido no representa la prueba del PCI correspondiente, sino que es una prueba de recuperación solamente del sistema TRAMIX en ambiente de contingencia –en este caso, nube AWS-.

Recomendación

Se deberá avanzar en medidas que permitan disponer de un Plan de Contingencia integral.

Para su consideración, está disponible la guía Plan de Contingencia, en el Banco de Metodologías de Trabajo del sitio web de SIGEN.

Dicho plan debe estar documentado y aprobado, probado periódicamente, mantenerse actualizado y transformarse en una parte integral del resto de los procesos de gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la organización y asegurar la reanudación oportuna de las operaciones y sistemas según su nivel de criticidad.

Considerar la necesidad de contar y definir un CPD Alternativo.

Asimismo, documentar la criticidad de los sistemas y establecer prioridades al momento de definir su resguardo y recuperación.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario:
"Sin comentarios."

Descripción del Curso de Acción a Seguir:
"- Elaboración del plan de contingencia en sintonía con el catálogo de activos de información.
- Definir procedimientos relacionados con las contingencias.
- Definir un CPD alternativo
- Documentar la criticidad de los sistemas y establecer prioridades al momento de definir su resguardo y recuperación."

***Fecha de Regularización Prevista**: "2do semestre 2024"*

Área o Sector Responsable: *"Responsable de Seg. Inf + Dirección de Ingeniería de Procesos + Dirección de Gestión de Usuarios y Red + Dirección de Informática + Gerencia de Organización y Sistemas"*

Comentario final SIGEN

El comentario del auditado responde a lo observado en el punto. No se efectúan comentarios adicionales.

5.11 GESTIÓN DE VULNERABILIDADES

Para la gestión de vulnerabilidades, el organismo **no cuenta con un procedimiento que regule esta práctica.**

Según lo informado, se utiliza Kaspersky desde 2018 para el antivirus, y respecto a los escaneos de vulnerabilidades, estos tendrían una frecuencia semanal. Adicionalmente, se destaca que un tercero (Consultora Vectus) ha realizado un análisis de vulnerabilidades sobre un sitio web y la intranet.

Respecto del ciberataque de tipo "ramsonware" sufrido por el CONICET el día 19 de abril de 2022, el auditado ha informado las siguientes acciones implementadas a raíz de ese incidente de seguridad:

- *"Restructuración de las tareas de la Gerencia,*
- *Reconstrucción de los ambientes de Windows.*
- *Apagado de sistemas de desarrollo y testeo, de manera preventiva.*
- *Formateo de PC y servidores, los cuales a la fecha se encuentran funcionando.*
- *Elevación de las medidas de seguridad en el firewall el cual actualmente cuenta con el firmware FortiOS 7.0.12 build 0523 (20/06/2023).*

- *Actualización de políticas de contraseña, se elevó el nivel de complejidad mínimo de las contraseñas para usuarios a 14 caracteres con obligatoriedad de mayúsculas, minúsculas, números y caracteres especiales. Para servicios críticos de administradores de sistemas se exigen certificados o contraseñas aún más robustas.*
- *Licitación de un servicio de consultoría de ciberseguridad para reforzar las medidas.*
- *Creación de un sitio web: https://www.conicet.gov.ar/seguridad-informacion/ junto con campañas de concientización para evitar futuros incidentes, creación de una casilla de email para la realización de consultas: seguridad.informacion@conicet.gov.ar."*

Por lo expuesto y por lo informado en relación a este punto, aún falta implementar suficientes medidas de seguridad para prevenir nuevos ataques.

Cabe agregar que el CONICET posee software obsoleto donde residen aplicaciones críticas, tema que se profundiza en el punto siguiente.

Recomendación

Documentar, aprobar e implementar el procedimiento para el registro de eventos o actividades sensitivas y su posterior revisión periódica por parte de un responsable, así como un procedimiento que defina el monitoreo periódico de incidentes de seguridad.

Planificar y realizar la ejecución de escaneos de vulnerabilidades en los servidores involucrados y la instalación de antivirus en los servidores, en conjunto con la revisión de las medidas de seguridad.

Implementar suficientes controles de ciberseguridad: sistemas de ciberseguridad biométrica, sistemas de análisis de tráfico de red en tiempo real, Firewalls o cortafuegos, Sistema de prevención de intrusiones IPS, Scanner de vulnerabilidades de aplicaciones web, antispam, Redes Virtuales Privadas (VPN), hacking ético, entre otros.

Asegurar que todo el software donde procesan los sistemas críticos cuenten con los parches de seguridad adecuados y protegido de amenazas y ciberataques.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

☐ De acuerdo
■ Parcialmente de acuerdo
☐ En desacuerdo

Comentario:
"Las vulnerabilidades mencionadas no tienen en consideración ningún aspecto de la arquitectura de seguridad. La red se encuentra segmentada en capa 2 y capa 3. Los servicios expuestos a los usuarios ya sean estos externos o internos en su gran mayoría se encuentran

detrás de servidores web Apache los cuales están permanentemente siendo actualizados. Para cruzar entre segmentos de red se debe necesariamente atravesar el firewall, el cual tiene configuradas todas las políticas/reglas de seguridad del organismo, y se encuentra actualizado. La actividad de los usuarios que acceden a sistemas productivos con privilegios especiales es monitoreada."

Descripción del Curso de Acción a Seguir:
"- Formalizar en un proyecto todas las actividades relacionadas a la gestión de vulnerabilidades y medidas de seguridad, de forma tal de facilitar su control, trazabilidad y visibilidad.
- Formalizar un documento donde se detallen todos los servicios de red accesibles por los usuarios internos y externos, y su esquema de seguridad / análisis de riesgos.
- Actualizar el software eventualmente donde se considere necesario sujeto a disponibilidad presupuestaria."

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: *"Dirección de Gestión de Usuarios y Red"*

Comentario final SIGEN

Los cursos de acción a seguir mencionados por el auditado se encuentran alineados a la recomendación de SIGEN. Según la respuesta del auditado, el CONICET se encuentra adoptando medidas en cuanto a lo observado, aspectos sobre los cuales se toma nota.

5.12 GESTIÓN DE INVENTARIO DE HARDWARE Y SOFTWARE

El auditado **no cuenta con un inventario formal de software y hardware ni procedimientos que regulen esta práctica,** razón por la cual SIGEN le proporcionó una planilla para que el auditado complete el detalle de todos los sistemas informáticos que posee el CONICET.

De acuerdo a lo informado por el auditado, desde 2015 utilizan una herramienta de código abierto denominada GLPi *(Gestionnaire Libre de Parc Informatique)*, para registrar el inventario de hardware y el software**. Sin embargo, a la fecha el organismo no concentra todo sus activos en esa herramienta, a efectos de constituir un inventario de hardware y software completo gestionado mediante un procedimiento formal que regule esta práctica.**

Por otro lado, el auditado ha listado los siguientes softwares que **no han sido incluidos en la planilla anteriormente mencionada**, indicando la modalidad de su licencia:

Licencias perpetuas:	Modalidad suscripción:	Licencias a perpetuidad sin costo:
•-VmWare, Windows Server •-Windows 10 •-Paquete Office •- SQL server •- Oracle •- MySql	•- Zoom •- Antivirus (Kaspersky) •- Atlas ti •- Firewall •- Power BI •- Adobe Creative Cloud •- Autocad •- Enterprise Architect •- Bejerman •- Reiwin •- Ableton Live	•- GitLab •- Software R

De lo expuesto, se agrega la siguiente información relevada, que no se encuentra claramente identificada en la documentación técnica remitida:

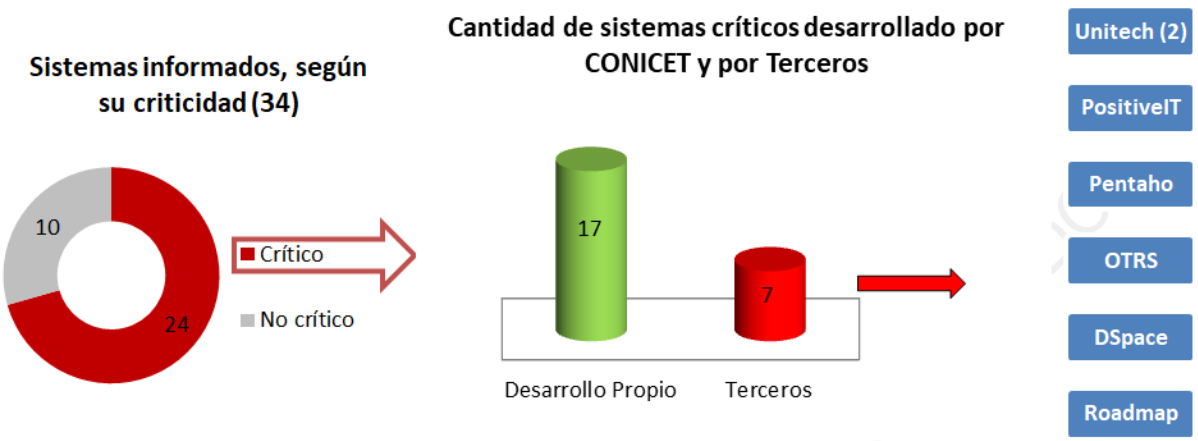
- Desde el CONICET CENTRAL se gestionan los activos de información del organismo, se desarrollan las tareas del personal administrativo mediante una infraestructura de virtualización de escritorios (VMware - Windows) y se desarrollan las diversas actividades mediante una infraestructura de virtualización de servidores (OpenStack - Linux).

- El sistema BACULA, no se incluye en ninguno de los inventarios internos remitidos.

Cabe hacer mención que en el "*Plan estratégico de TI 2023 – 2025.pdf*" remitido, surge un proyecto que consiste en desarrollar un Inventario de activos de información. **Sin embargo no se obtuvo documentación al respecto.**

Según la planilla completada por el auditado *"Detalle de todos los sistemas que posee el CONICET.xls"*, surge que:

- Se informan 34 sistemas activos, de los cuales 25 son desarrollados por éste, siendo 17 críticos, los 9 restantes corresponden a sistemas de terceros, de los cuales 7 son críticos.



- **No se pudo tomar conocimiento sobre la ubicación de los sistemas reportados, es decir si residen en el CPD del Organismo o en un tercero, de corresponder.**

Obsolescencia

Sistemas desarrollados por terceros:

Para mayor entendimiento, se adjunta extracto:

Sistemas desarrollados por terceros	Proveedor	Manuales usuario	Manuales técnicos	Versión Base de datos	Versión Sistema Operativo
CRM - CRM de la Gerencia de Vinculación Tecnológica	PositiveIT	√	No	MySQL 5.6.27	*CentOS 7.9 (vence en 2024)*
Datawarehouse	Pentaho	√	√		
ENCUE - Encuestas	LimeSurvey	√	No		
Moodle - Capacitación	Moodle	√	√		
OTRS - Ticketera	OTRS	√	√		
DSpace	DSpace	√	√		
PGD - Sistema de Planes de Gestión de Datos	Roadmap	√	No	PostgreSQL 9.6	
Tramix Liquidación de Haberes	Unitech	√	√	Oracle 11.2.0.2	Oracle Linux Server 6.10.0
Integrador TramixLH - Sigerh		No	√		

Todos los sistemas considerados críticos (en negrita) procesan en versiones de software obsoletas (en rojo) o próximas a finalizar su soporte (en amarillo).

Sistemas desarrollados por CONICET:

	Sistemas desarrollados por CONICET	Manuales usuario	Manuales técnicos	Versión Base de datos	Sistema Operativo
1.	ACC - Ayuda Consultas Carrera	No	No	MySQL 5.6.27	*CentOS 7.9 (vence en 2024)*
2.	Agenda	√	√		
3.	ARH - Ayuda Recursos Humanos	No	No		
4.	CIFRAS - CONICET CIFRAS	√	√		
5.	ECO - Economato	No	No		
6.	MEC - Mesa de Entrada	√	√		
7.	SIDO - Sistema de Información Documental	√	√		
8.	WPANC - Notables de la Ciencia	√	√		
9.	**BICYT - Buscador Integral de Ciencia y Tecnología**	√	No		
10.	**ELEC - Elección**	√	√		
11.	**SIGEVA - Sistema Integral de Gestión y Evaluación**	√	√		
12.	**Intranet CONICET**	√	√		
13.	**IUI - Identificación Usuario Intranet**	√	√		
14.	**RI - Repositorio Institucional**	√	No		
15.	**SIAF - Sistema Integral de Administración de Financiamientos**	√	√		
16.	**SIAF-AGF - Autogestión de Fondos**	√	√		
17.	**SIBI - Sistema informático de bienes inventariables**	√	√		
18.	**SIGEF - Sistema Integral de Gestión de Fondos**	√	√		
19.	**SIGEO - Sistema Integral de Gestión de Organizaciones**	√	√		
20.	**SINE - Sistema Integral de Notificaciones Electrónicas**	√	√		
21.	**SVT - Sistema de Vinculación y Convenios**	√	√		
22.	**INTWEB - Correo**	√	√		

Sistemas desarrollados por CONICET	Manuales usuario	Manuales técnicos	Versión Base de datos	Sistema Operativo
23. Portal Multisitio	√	√		
24. Hostings SIGEVA	√	√		
25. SIGERH - Sistema Integral de Gestión de Recursos Humanos	√	√	MySQL 5.6.27 Oracle 11 SQLServer 2016	*CentOS 7.9*

- 25 sistemas son desarrollos por CONICET, de los cuales 17 son considerados críticos. **Todos estos sistemas procesan en versiones de software obsoletas (resaltada) o próximas a finalizar su soporte (CentOS).**

- **Inconsistencias en la documentación y nomenclatura de los sistemas. Los sistemas informados en la planilla remitida difieren en cantidad y nomenclatura con los incluidos en el Plan informático estratégico y Plan de Contingencia.** Para más información, remitirse a los puntos 4.1, 5.6 y 5.10 respectivamente.

Adicionalmente, el CONICET **carece de un procedimiento formal de gestión y control de licencias de software.**

Recomendación

Se sugiere formalizar un inventario formal de hardware y software que reúna los detalles técnicos antes mencionados y se concentre la información, de ser posible, en una única herramienta.

Completar la información que contiene el inventario de servidores, indicando principalmente el entorno de procesamiento, qué herramienta se encuentran dando servicio, en qué ambiente y en qué CPD se aloja, de corresponder.

Desarrollar un procedimiento formal para la gestión y control de licencias de software y aprobarlo por la autoridad.

Las licencias deben estar formalizadas. Se sugiere propiciar que las versiones cuenten con el soporte del proveedor correspondiente, a fin de obtener el rendimiento correcto en los servidores donde residen las aplicaciones críticas del Organismo (por ejemplo, TRAMIX).

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario: *"Sin comentarios"*

Descripción del Curso de Acción a Seguir:
"- Completar el inventario de hardware y software.
- Desarrollar un procedimiento formal para la gestión y control de licencias de software y aprobarlo por la autoridad."

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: *"Dirección de Gestión de Usuarios y Red"*

Comentario final SIGEN

El comentario del auditado responde parcialmente a lo observado en el punto. Se reitera tomar acción sobre la obsolescencia de software detectada en los servidores que procesan sistemas críticos.

5.13 DOCUMENTACIÓN TÉCNICA Y FUNCIONAL DE LOS SISTEMAS UTILIZADOS EN EL CONICET

Según la planilla completada por el auditado *"Detalle de todos los sistemas que posee el CONICET.xls"*, surge que:

- Sistemas desarrollados por terceros:
    - **2 sistemas críticos carecen de sus manuales técnicos (CRM, PGD).**
    - **1 sistema no crítico carece de su manual técnico (ENCUE).**
    - **1 sistema crítico carece de su manual de usuario (Integrador TramixLH - SIGERH)**
- Sistemas desarrollados por CONICET:
    - **3 sistemas no críticos carecen de sus manuales técnicos y de usuarios (ACC - Ayuda Consultas Carrera, ARH - Ayuda Recursos Humanos, ECO - Economato).**
    - **2 sistemas críticos carecen de su manual técnico (BICYT - Buscador Integral de Ciencia y Tecnología, RI - Repositorio Institucional)**

Recomendación

Documentar y consolidar toda la documentación técnica y funcional del sistema bajo análisis, especificando los módulos con su descripción y funcionalidad y las interfaces que tienen vinculación con el mismo, la cual tiene que formar parte de la documentación general del sistema.

Opinión del Auditado, curso de acción a seguir y área o sector responsable

- ■ De acuerdo
- ☐ Parcialmente de acuerdo
- ☐ En desacuerdo

Comentario: *"Sin comentarios"*

Descripción del Curso de Acción a Seguir: *"- Completar la documentación faltante para los sistemas críticos."*

Fecha de Regularización Prevista: *"2do semestre 2024"*

Área o Sector Responsable: *"Dirección de Informática"*

Comentario final SIGEN

El comentario del auditado responde a lo observado en el punto. No se efectúan comentarios adicionales.

6 CONCLUSIONES

La labor presentada en este informe corresponde a la auditoría realizada respecto de los Controles Generales de Tecnología Informática, en particular a la gestión de resguardo y recuperación de la información del CONICET.

De la auditoría realizada, surgieron aspectos que ameritan ser observados, según se expuso detalladamente en los puntos precedentes del presente informe, sobre los que se han formulado recomendaciones orientadas a reducir los riesgos asociados.

En ese orden, se recomendó adoptar medidas respecto a la organización del área de Tecnología de la Información en cuanto a sus responsabilidades, misiones y funciones, así como contar con un plan informático que contemple todos los aspectos de control asociados a la ejecución y seguimiento de proyectos informáticos.

En ese mismo sentido, se recomendó desarrollar e implementar los procedimientos faltantes (gestión de usuarios, registro, revisión y monitoreo de logs, licencias de software, seguridad física, cambios a programas/jobs/scripts, registro y monitoreo de incidentes, vulnerabilidades, entre otros) y actualizar los procedimientos existentes (gestión de usuarios, resguardo y recuperación de la información, entre otros). Documentar la evidencia de su aprobación e indicar sus fechas de vigencia.

De igual forma, se recomendó culminar el desarrollo de un Plan de Contingencias formal, con el detalle de los procedimientos de recuperación por sistema crítico, entre otros y definir un centro de procesamiento alternativo que cuente con suficientes medidas de seguridad.

Respecto a la gestión de resguardo y recuperación de la información, se insta a actualizar el procedimiento interno incorporando las acciones de la práctica actual, e incluyendo los aspectos que detalla el plan contenido en el Anexo del presente informe. Promover su aprobación por parte de la autoridad, indicando su fecha de vigencia, y su implementación. Asimismo, y complementándolo, documentar formalmente el criterio para clasificar los activos y/o utilizar una metodología aprobada, a modo de establecer la criticidad de los mismos y establecer prioridades al momento de definir su resguardo y recuperación.

Al respecto, se sugiere mejorar las condiciones del establecimiento donde se resguardan actualmente las copias de seguridad en sitio externo.

Respecto a las observaciones identificadas, el CONICET ha encarado acciones para diversos señalamientos y ha formulado cursos de acción alineados a las recomendaciones efectuadas por SIGEN, estableciendo responsables y plazos para las medidas a instrumentar, lo que permitirá reducir los riesgos que surgen de los aspectos observados. Al respecto, se sugiere efectuar el oportuno seguimiento de dicho plan de acción, requiriendo por su parte, sea completado en relación a los puntos faltantes.

Buenos Aires, noviembre de 2023

ANEXO

Programa de trabajo elaborado por SIGEN: *"Guía para la revisión del proceso de gestión de resguardo y restauración de la información*", a efectos de que pueda ser utilizado como elemento de autoevaluación en las etapas subsiguientes del desarrollo del Plan.

Guía para la revisión del proceso de gestión de resguardo y restauración de la información								
OBJETIVOS DE CONTROLES	**DESCRIPCIÓN**	**ASPECTOS A VERIFICAR**	**Si**	**No**	**Parc**	**COMENTARIOS/ OBSERVACIONES**	**Ref. Pap. de trab.**	**Obs. en INFORME**
1. CONSIDERACIONES GENERALES								
1.1 EXISTENCIA DE UNA POLÍTICA DE SEGURIDAD Y SU VINCULACIÓN CON LA CONTINUIDAD OPERATIVA	El Organismos debe contar con una **Política de Seguridad de la Información** aprobada por la autoridad y debe estar alineada a las normas complementarias o modificatorias.	¿Se posee una Política de Seguridad de la Información aprobada y alineada a la normativa vigente?						
		¿La Política de Seguridad de la Información detalla lineamientos asociados a la continuidad operativa, en particular a la gestión de resguardo y restauración de la información?						
	Los **Planes de Contingencia** informática son una parte de los Planes de Continuidad del Negocio/Actividad donde se establecen las respuestas o tratamiento de las incidencias o contingencias.	¿El Organismo cuenta con un Plan de Contingencia aprobado?						
2. PROCEDIMIENTO DE RESGUARDO Y RESTAURACIÓN DE LA INFORMACIÓN								
2.1 GESTIÓN DE RESGUARDO Y RESTAURACIÓN DE LA INFORMACIÓN	El organismo debe asegurarse la disponibilidad e integridad de la información, ante incidentes y en caso de contingencia, efectuando copias de seguridad de la información mediante un **procedimiento formal** que regule esta práctica. El procedimiento debe estar **aprobado** por la autoridad y debe alinearse a los lineamientos que se desprenden de la Política de Seguridad de la Información.	¿Existe un procedimiento documentado y aprobado para la gestión de resguardo y restauración de la información?						
	El procedimiento debe incluir el círcuito o pasos a seguir del proceso, el objetivo, alcance, responsabilidades, normativa aplicable, conceptos generales, usuarios claves del proceso, aspectos de control claves, las referencias a documentos relacionados al mismo, diagramas para el entendimiento (opcional), historial de versiones, aprobador, revisor y los siguientes aspectos de control que se exponen a continuación:	¿El procedimiento incluye el circuito o pasos a seguir del proceso, los aspectos de control claves, objetivo, alcance, responsabilidades, normativa aplicable, conceptos generales, usuarios claves del proceso, referencias a documentos relacionados al mismo, diagramas para el entendimiento (opcional), historial de versiones, aprobador, revisor?						

Guía para la revisión del proceso de gestión de resguardo y restauración de la información								
OBJETIVOS DE CONTROLES	**DESCRIPCIÓN**	**ASPECTOS A VERIFICAR**	**Si**	**No**	**Parc**	**COMENTARIOS/ OBSERVACIONES**	**Ref. Pap. de trab.**	**Obs. en INFORME**
3. SISTEMAS/SERVICIOS CRÍTICOS								
3.1 CLASIFICACIÓN DE LOS ACTIVOS SISTEMAS/SERVICIOS CRÍTICOS	Se debe implementar un **sistema de clasificación de los activos de información** que permita identificar cuestiones como el nivel de protección requerido, el tipo de activo, su criticidad y por consecuencia su prioridad.	El procedimiento ¿se basa en un análisis documentado en que se hayan definido los **datos y sistemas críticos y su prioridad de recuperación**?						
	Se deben definir los sistemas críticos con su prioridad de restauración para ello se debe considerar la relación o **dependencia técnica** que mantienen los sistemas críticos entre sí, ya sea lógica como físicamente.	¿Los sistemas críticos tienen **dependencia técnica** entre ellos?						
	Es conveniente que el diseño e implementación de un **sistema de clasificación de activos de información,** se efectué mediante una **metodología** diseñada para tal fin.	¿Se posee una **metodología formal para clasificar e implementar un sistema de clasificación de activos**?						
	Una vez efectuada la clasificación de los activos, según metodología, se debe realizar un **inventario de activos** que permita: Identificar los activos de información que dan soporte a la actividad; Clasificar los activos por su importancia **(prioridad);** Clasificar los activos por el tipo de activo o información; Identificar al propietario del activo (información), entre otros.	¿Cuenta con un **inventario formal de los activos de información relativos a los servicios y sistemas**?						
		¿Las **prioridades de restauración** se encuentran formalmente **documentadas**?						
	A modo de ejemplo: *Identificación del equipo físico o virtual; Servicio prestado por el/los equipo/s; Nombre del Activo/Sistema/Descripción;* o *Entorno tecnológico; Ubicación lógica del conjunto de archivos a resguardar; Tamaño aproximado de los datos a resguardar; Responsable de Infraestructura; Responsable técnico del activo de información; Dueño de la información, entre otros.*	¿Se utiliza una **herramienta para la gestión de inventarios** de hardware y software?						
	El **inventario de activos** debe mantenerse **actualizado,** y cada cambio en el mismo debe ser aprobado formalmente. Asimismo, debe **revisarse periódicamente** a fin de verificar que no existan datos críticos que no se estén resguardando.	Ante un cambio en los activos de información a resguardar, se gestiona el mismo a través de una solicitud que contemple todas las autorizaciones correspondientes?						
		¿El **inventario se mantiene actualizado y revisado periódicamente** a modo de asegurar que todos los datos críticos se resguarden adecuadamente?						

Guía para la revisión del proceso de gestión de resguardo y restauración de la información								
OBJETIVOS DE CONTROLES	**DESCRIPCIÓN**	**ASPECTOS A VERIFICAR**	**Si**	**No**	**Parc**	**COMENTARIOS/ OBSERVACIONES**	**Ref. Pap. de trab.**	**Obs. en INFORME**
4.1 RESPONSABLES DEL RESGUARDO/RESTAURACIÓN DE COPIAS DE SEGURIDAD	Se debe incluir en el procedimiento formal los **responsables** de llevar a cabo los resguardos/recuperación y todas las tareas en relación a esta gestión.	¿Se encuentran formalmente asignados los responsables de ejecutar las actividades de resguardo y restauración?						
		¿Los **agentes** definidos son los designados?						
4.2 ALCANCE COPIAS DE SEGURIDAD	Las copias de seguridad deben tener un **alcance** adecuado para cubrir las necesidades de resguardo de su información: - Datos e información sensible. - Software y aplicaciones. - Datos de configuración de aplicaciones, sistemas, etc. - Datos sobre accesos, claves, etc. - Registros de actividades, eventos, mensajes o alarmas del sistema.	¿Se encuentra definido formalmente en el procedimiento el alcance que deben tener las copias de seguridad? Señale que tipos abarca [X]: - Datos e información sensible. [ ] - Software y aplicaciones. [ ] - Datos de configuración de aplicaciones, sistemas, etc. - Datos sobre accesos, claves, etc.[ ] - Registros de actividades, eventos, mensajes o alarmas del sistema.[ ]						
4.3 TIPOS DE COPIAS DE SEGURIDAD	Se debe decidir el tipo de copia adecuada para cada uno de los sistemas/ servicios **críticos** en el procedimiento, estimando cuestiones como los responsables, recursos y medios de almacenamiento. A modo de ejemplo, existen distintos tipos de resguardos: a. Completa: se copian el total de los datos. b. Incremental: solo se guardan los datos modificados desde la última copia. c. Diferencial: se guardan todos los datos modificados desde la última copia completa. Existen otros tipos: resguardo incremental inverso, espejo, sintética completa, entre otros.	¿Se encuentran definidos los tipos de copias, recursos y responsables en el procedimiento de gestión de resguardo y restauración de la información, por cada sistema/servicio crítico?						
4.4 PERIODICIDAD DE LAS COPIAS DE SEGURIDAD	Se debe estipular y fijar la **frecuencia** con la cual se realizarán las copias de seguridad, a través de un **esquema de resguardo**, teniendo en cuenta factores tales como: a. Criticidad de los datos b.Cantidad y tiempo de variación estimada de los datos a guardar c. Costo del almacenamiento d. Servicios e infraestructuras afectadas e. Obligaciones legales	¿El **esquema de resguardo** (cronograma de resguardos) se encuentra formalizado en el procedimiento?						
		La **periodicidad del resguardo** ¿es razonable considerando la criticidad de los datos?						

Guía para la revisión del proceso de gestión de resguardo y restauración de la información								
OBJETIVOS DE CONTROLES	**DESCRIPCIÓN**	**ASPECTOS A VERIFICAR**	**Si**	**No**	**Parc**	**COMENTARIOS/ OBSERVACIONES**	**Ref. Pap. de trab.**	**Obs. en INFORME**
4.5 CIFRADO EN LAS COPIAS DE SEGURIDAD	Para el respaldo y protección de información, se recomienda la **encriptación** de las copias de seguridad a fin de adicionar una capa adicional de seguridad y garantizar que todos los datos permanecen inalterables mientras se encuentran almacenados.	¿Las copias de seguridad se encuentran **encriptadas?**						
4.6 REGISTROS (LOGS) EN LA EJECUCIÓN DEL RESGUARDO	El proceso de copia de seguridad debe generar un **registro de ejecución u operación (log)** que permita la revisión del resultado de la ejecución.	¿Los procesos de resguardo generan un **registro en el log** con el resultado de su ejecución?						
	Los **logs** deben ser resguardados del personal no autorizado.	¿Los logs son protegidos de **accesos no autorizados**?						
5. MEDIOS/SOPORTE DE ALMACENAMIENTO								
5.1 TIPO DE MEDIOS DE ALMACENAMIENTO Y MANTENIMIENTO	Los medios en los que se resguardan las copias deben contar con el **mantenimiento adecuado** en pos de permitir la restauración de las copias de seguridad. A modo de ejemplo: Cintas magnéticas, Discos duros HDD y SSD, **Nube.**	¿Para los medios de almacenamiento utilizados, existe un **plan de mantenimiento preventivo**?						
5.2 ROTULACIÓN DE LAS COPIAS DE SEGURIDAD Y SUS MEDIOS	Definir un **esquema de rotulado de las copias de resguardo,** que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.	¿Se cuenta con un **procedimiento para el rotulado** de las copias de resguardo y su medio de almacenamiento?						
5.3 DESTRUCCIÓN DE LOS MEDIOS	Cuando sea necesario la **destrucción** del medio que almacenó alguna de las copias de seguridad, ésta debe realizarse de forma segura, con un procedimiento que garantice que la información que contuvo no pueda volver a ser accesible.	¿Existe un procedimiento que garantice que, al momento de destruir, desafectar o reutilizar medios de almacenamiento, la información que contuvo **no pueda volver a ser accesible**?						
	Se debe establecer un **esquema de reemplazo** de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo con lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.	¿Existe un **esquema de reemplazo** de los medios de almacenamiento de las copias de resguardo?						
6. UBICACIÓN COPIAS DE SEGURIDAD / RESGUARDOS								
6.1 ESTRATEGIAS DE REALIZACIÓN DE COPIAS DE SEGURIDAD - UBICACIONES ALTERNATIVAS	Se debe implementar **una estrategia de resguardo** que tienda a garantizar continuidad operativa ante posibles contingencias. A modo de ejemplo: Estrategia *3-2-1. Consiste en mantener al menos 3 copias de los datos y toda la información* ***relevante.*** *Las copias deben almacenarse en al menos 2 medios/soportes distintos, y al menos una copia de seguridad debe estar almacenada* ***en sitio externo,*** *fuera del Centro de Procesamiento.*	¿Se encuentra documentada formalmente la estrategia de resguardo seleccionada para asegurar la recuperación de los datos en caso de desastres?						
		¿El Centro de Procesamiento donde se procesan y se alojan las copias de seguridad cuenta con suficientes medidas de seguridad?						

Guía para la revisión del proceso de gestión de resguardo y restauración de la información								
OBJETIVOS DE CONTROLES	**DESCRIPCIÓN**	**ASPECTOS A VERIFICAR**	**Si**	**No**	**Parc**	**COMENTARIOS/ OBSERVACIONES**	**Ref. Pap. de trab.**	**Obs. en INFORME**
		Las copias de seguridad ¿**se almacenan en un sitio externo**?						
	Se debe establecer la **periodicidad** del resguardo también en **sitio externo,** considerando la criticidad de los datos.	¿La **periodicidad** del resguardo en **sitio externo es razonable** considerando la criticidad de los datos?						
6.2 SEGURIDAD FÍSICA Y DE ACCESO A LOS MEDIOS/SOPORTES EN SITIO EXTERNO	Las cintas de seguridad deben ubicarse en un **lugar de protección física y ambiental** adecuada para mantener la confidencialidad, la integridad y la disponibilidad de la información, de software y sistemas informáticos	¿Las **cintas se encuentran debidamente protegidas en el sitio externo**?						
	El sitio donde se almacenan y resguardan las copias de seguridad debe estar **restringido al acceso de personal no autorizado.**	¿El **sitio externo es de acceso restringido?**						
6.3 TRASLADOS SEGURO AL SITIO EXTERNO	Se deben registrar l**os ingresos y egresos de los autorizados a trasladar las copias de seguridad, día y horario de dichos eventos**, y cualquier otro dato que ayude a garantizar la seguridad de las mismas, incluyendo su trazabilidad.	¿Existe un p**rocedimiento para el traslado seguro de copias de seguridad**, donde se contemple el registro de entrada/salida de las cintas, las autorizaciones correspondientes, los requisitos que deben acompañar las copias de seguridad, entre otros?						
7. PROCEDIMIENTOS DE RESTAURACIÓN O RECUPERACIÓN								
7.1 ACTIVIDADES DE RESTAURACIÓN DE LA INFORMACIÓN	Se refiere a la restauración total o parcial de la información original que se encuentra protegida en el medio o soporte de almacenamiento. Los medios de restauración y el sistema de copias de seguridad deberían permitir restauraciones parciales del sistema dependiendo de las distintas aplicaciones y sistemas de forma que un incidente o contingencia de un sistema o aplicación no obligue a la restauración de otras aplicaciones con el consiguiente impacto.	¿Existe un **procedimiento formal para la restauración de los sistemas críticos** ante una posible contingencia o incidente?						
		¿Los medios de restauración y el sistema de copias de seguridad contemplan las **restauraciones parciales**?						
7.2 PRUEBAS DEL PROCEDIMIENTOS DE RESTAURACIÓN	Es necesario fijar un **período para realizar pruebas de restauración de las copias de seguridad formales,** corroborar el adecuado estado de los distintos medios/soportes de almacenamiento utilizados y la efectividad de los procesos destinados a tal fin.	¿Se **prueban periódicamente los procedimientos de restauración** garantizando su eficacia y cumplimiento en el tiempo asignado a la restauración en los procedimientos operativos?						
		¿Todas las **pruebas efectuadas son documentadas**, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos?						

Guía para la revisión del proceso de gestión de resguardo y restauración de la información								
OBJETIVOS DE CONTROLES	**DESCRIPCIÓN**	**ASPECTOS A VERIFICAR**	**Si**	**No**	**Parc**	**COMENTARIOS/ OBSERVACIONES**	**Ref. Pap. de trab.**	**Obs. en INFORME**
		¿Se indica quienes son los **responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido**?						
		¿Se ha establecido un **cronograma de pruebas periódicas**?						
		¿Se establecen los **métodos de la prueba**? Por ejemplo: muestreo, entre otros.						
8. SISTEMA INFORMÁTICO DE RESGUARDO Y RESTAURACIÓN - ALERTAS POR FALLAS EN LOS PROCESOS								
8.1 USO DE UN SISTEMA INFORMÁTICO DE RESGUARDO Y RECUPERACIÓN DE LA INFORMACIÓN **CREACIÓN DE JOBS (TAREAS AUTOMATIZADAS DE RESGUARDO Y RECUPERACIÓN)**	Debe utilizarse un **sistema informático** para generar los resguardos que se encargue de hacer un plan de copias y ejecutar los resguardos o restauraciones, según la programación.	¿Se utiliza un **sistema informático** para generar los resguardos y las restauraciones?						
	Se debe efectuar la **actualización del sistema de resguardo** (software/hardware/), cuando sea necesario. Asimismo, se debe efectuar el resguardo de la información del mismo.	¿El sistema se encuentra **actualizado y reside en servidores cuyas versiones de software cuentan con el soporte de seguridad correspondiente?** ¿Existen **copias de seguridad del sistema de resguardo y recuperación**?						
	La **creación de los Job** deben documentarse, probarse, autorizarse y aprobarse su ejecución en producción por parte de la autoridad. Es importante que cuando se configuren o programen los Jobs también se programen las notificaciones, ante fallas en su ejecución.	¿Se crean las tareas automatizadas (Job) en el sistema de resguardo y recuperación respetando los **criterios establecidos en el inventario y procedimiento**?						
		Ante una **modificación** en las **tareas de resguardo**s o al momento de la **creación** de una nueva tarea, ¿**se verifica la correcta ejecución de la misma**?						
		Una vez ejecutado el resguardo ¿se **verifica que la tarea de resguardo no haya arrojado errores o advertencias** (warnings)?						
8.2 VERIFICACIÓN PERIÓDICA DE LA INFORMACIÓN DEL SISTEMA	Se debe **revisar toda la información de este sistema periódicamente** a fin de poder efectuar estimaciones en cuanto a: almacenamiento, opciones de recuperación, escalabilidad, performance, entre otras.	¿Se **revisa la información del sistema en forma periódica**?						
8.3 VERIFICACIÓN PERIÓDICA DE LOS ACTIVOS A RESGUARDAR	Se debe verificar que **todos los activos de información "críticos"** están incluidos en la configuración y se están copiando.	¿El sistema procesa todos los Jobs que resguardan los activos de información?						

Guía para la revisión del proceso de gestión de resguardo y restauración de la información								
OBJETIVOS DE CONTROLES	**DESCRIPCIÓN**	**ASPECTOS A VERIFICAR**	**Si**	**No**	**Parc**	**COMENTARIOS/ OBSERVACIONES**	**Ref. Pap. de trab.**	**Obs. en INFORME**
8.4 GESTIÓN DE NOTIFICACIONES Y GESTIÓN DE INCIDENTES	Se debe implementar un **sistema de notificaciones** que alerte al personal de mantenimiento sobre el estado de la ejecución de los procesos de resguardo y recuperación, incluidas fallas completas o parciales, para que se puedan tomar medidas correctivas. Una buena práctica es **generar un incidente** para resolver errores producidos del proceso de resguardo y/recuperación.	Ante errores, ¿se generan **incidentes en una herramienta** destinada para ese fin?						
		¿Ante un error en las tareas de resguardo el sistema da **aviso a los responsables para su resolución**?						

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Informe de Auditoría Reservado

Número: IF-2023-136777682-APN-GCPE#SIGEN

CIUDAD DE BUENOS AIRES
Jueves 16 de Noviembre de 2023

Referencia: Informe de Auditoría – Controles de la Gestión de la Tecnología de la Información -CONSEJO NACIONAL DE INVESTIGACIONES CIENTÍFICAS Y TÉCNICAS -CONICET.

El documento fue importado por el sistema GEDO con un total de 70 pagina/s.

Karina SIlvina Cotoia
Coordinadora
Gerencia de Control de Proyectos Especiales
Sindicatura General De La Nación

Sandra Rita Vaccarezza
Subgerente
Gerencia de Control de Proyectos Especiales
Sindicatura General De La Nación

Marina Lucia VARELA
Gerente
Gerencia de Control de Proyectos Especiales
Sindicatura General De La Nación