POR EL CUIDADO Y BUEN USO
DE LOS RECURSOS PÚBLICOS

CONTRALORIA REGIONAL DE ARICA Y PARINACOTA

UNIDAD DE CONTROL EXTERNO

INFORME FINAL

UNIVERSIDAD DE TARAPACÁ

INFORME N° 68/ 2023

29 DE ABRIL DE 2025

OBJETIVOS
DE DESARROLLO
SOSTENIBLE

OBJETIVOS DE DESARROLLO SOSTENIBLE

9 INDUSTRIA, INNOVACIÓN E INFRAESTRUCTURA

16 PAZ, JUSTICIA E INSTITUCIONES SÓLIDAS

CONTRALORÍA GENERAL DE LA REPÚBLICA CHILE

POR EL CUIDADO Y BUEN USO DE LOS RECURSOS PÚBLICOS

INDICE

RESUMEN EJECUTIVO 1
JUSTIFICACIÓN 3
ANTECEDENTES GENERALES 3
OBJETIVO 4
METODOLOGÍA 4
UNIVERSO Y MUESTRA 5
RESULTADO DE LA AUDITORÍA 5
I. ASPECTOS DE CONTROL INTERNO 5
1. Sistema sin actualizar 6
II. EXAMEN DE LA MATERIA AUDITADA 7
2. Encargado de Seguridad. 7
3. Gestión de Riesgo. 8
4. Política de Seguridad 9
5. Comité de Seguridad. 10
6. En cuanto a la validación de equipos 11
6.a Equipos no encontrados. 11
6.b En cuanto al control de Inventario. 12
6.c En relación con las hojas de vida. 13
6.d Responsable y ubicación de equipos. 15
7. Activos sin registro de custodio en información entregada. 16
8. Respecto a la Sala de Servidores 17
8.a Seguridad Física de la Plataforma 17
8.b Controles Ambientales 18
8.c Suministro de Energía 18
8.d Compra y Mantención de Arquitectura Tecnológica 20
9. Procedimiento de destrucción de información. 21
10. Sociabilización de la política. 21
11. Rol de administrador en perfiles de usuario. 22
12. En cuanto al control de acceso a los equipos 24
13. Integridad de Respaldos. 25

14. Política de Control de Acceso.....26
15. Política interna de Control de Acceso.....27
16. Estructura de Contraseñas.....31
17. Usuarios desvinculados activos en sistema.....31
18. Control de Acceso Remoto.....32
19. Control de Acceso lógico para VPN.....33
20. Sobre los Softwares instalados.....34
20.a Programa Winrar.....34
20.b Programas sin activar.....34
20.c Programa sin Licencia.....35
21. Creación del Plan de Contingencia.....36
22. Control de Valores.....37
CONCLUSIONES.....38
Anexo N° 1: Equipos no encontrados.....43
Anexo Nº 2: Equipos sin custodio.....44
Anexo N° 3: Estado de Observaciones de Informe Final N° 68, de 2023.....47

RESUMEN EJECUTIVO
Informe Final N° 68, de 2023
Universidad de Tarapacá

Objetivo: Efectuar una auditoría al Macroproceso de Tecnologías de la Información en la Universidad de Tarapacá, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por esa entidad, a través de la existencia y aplicación de políticas, normas y procedimiento de seguridad informática que permitan asegurar la integridad, confiabilidad y confidencialidad de la información en sus sistemas informáticos y redes de comunicación, conforme a las Normas Técnicas aplicables para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, aprobada por el artículo primero del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia.

Preguntas de la auditoría:

- ¿Ha implementado la Universidad de Tarapacá Controles que permitan asegurar la integridad de los sistemas informáticos?

Principales resultados:

- De indagaciones efectuadas, se determinaron diversas deficiencias en cuanto a los controles, a las estructuras de las contraseñas, incumplimientos a la política interna de control de acceso, lo que no se ajusta al decreto N° 83, de 2004 y al decreto exento Nº 187, de 2020, por lo que la universidad deberá remitir la documentación de respaldo que acredite la implementación de las medidas informadas en su respuesta, esto es, de la revisión y ajustes de los permisos de las cuentas locales, la implementación de disposiciones que: prohíban permisos administrativos en cuentas no autorizadas; requieran contraseñas robustas para todas las cuentas, que incluyan longitud mínima y combinación de caracteres especiales, números y letras; sobre su cambio en forma periódica; sobre la nomenclatura estandarizada para todas las cuentas de usuario que facilite la identificación y control de acceso; de la configuración del sistema que obligue a la creación de contraseñas al configurar nuevas cuentas; de la creación de cuentas específicas para tareas administrativas y de la eliminación de aquellas genéricas; de acceso especiales para terceros, del establecimiento de controles críticos para la instalación de software; de una solución de gestión de aplicaciones que controlen y supervisen la instalación de software; y del marco integral de controles internos de TI, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

- Se determinó que no existe la administración de perfiles de usuario y de un administrador de sistema, por lo que la UTA deberá remitir la política de control de acceso de la información actualizada, que abarque la materia indicada precedentemente, y el acto administrativo que designe al “administrador de dominio, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

- Se advirtió la existencia de programas sin licencia y sin activar, vulnerando lo establecido en la letra b) del artículo 22 del mencionado decreto N° 83, de 2004, y los artículos 19 y 20 de la ley N° 17.336, motivo por el cual la universidad deberá remitir los respaldos fotográficos que den cuenta de la desinstalación del programa Winrar de los equipos indicados en la tabla N° 7, y del software PhantomPDF, instalado en el bien individualizado con el código de inventario N° 53071228-3, y de la activación de las licencias de Microsoft office Profesional 2013 y Microsoft Visio 2016, de los computadores asociados al N° de inventario 53016016-1, y Nº 53071228-3, respectivamente, así como también, la política para monitorear y gestionar las licencias de forma continua, de acuerdo a su respuesta, debidamente sancionada, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ARICA Y PARINACOTA
UNIDAD DE CONTROL EXTERNO

SIM N° 15.039/2022
C.E. Nº 5/2024
REFS. N^OS 926.607/2024
926.643/2024

INFORME FINAL DE AUDITORÍA N° 68, DE 2023, SOBRE AUDITORÍA AL MACROPROCESO DE TECNOLOGÍAS DE LA INFORMACIÓN, EN LA UNIVERSIDAD DE TARAPACÁ

Arica, 29 de abril de 2025

En cumplimiento del plan anual de fiscalización de esta Contraloría Regional de Arica y Parinacota, y en conformidad con lo establecido la ley N° 10.336, de Organización y Atribuciones de la Contraloría General de la República, se efectuó una auditoría al macroproceso de Tecnologías de la Información, en la Universidad de Tarapacá, por el período comprendido entre el 1 de enero de 2021 y el 31 de diciembre de 2021.

JUSTIFICACIÓN

A partir de la ejecución de auditorías de sistemas desarrolladas por esta Contraloría General de la República, se han advertido deficiencias en los sistemas informáticos mantenidos por los servicios públicos y municipalidades que conforman la Administración del Estado, que afectan la seguridad y confiabilidad de estos. Asimismo, en los últimos años se han conocido públicamente ataques que han afectado el normal funcionamiento de estos sistemas, por lo que, resulta relevante evaluar el nivel de seguridad implementado por las entidades.

Asimismo, a través de esta auditoría, la Contraloría Regional de Arica y Parinacota busca contribuir a la implementación y cumplimiento de los 17 Objetivos de Desarrollo Sostenible, ODS, aprobados por la Asamblea General de las Naciones Unidas en su Agenda 2030, para la erradicación de la pobreza, la protección del planeta y la prosperidad de toda la humanidad.

En tal sentido, esta revisión se enmarca en el ODS N°s. 16, Paz, Justicia e Instituciones Sólidas y 9, Industria, Innovación e Infraestructura.

ANTECEDENTES GENERALES

Como cuestión previa, mediante el decreto con fuerza de ley N° 150, de 1981, del Ministerio de Educación, se crea la Universidad de Tarapacá, fusionando el Instituto Profesional de Arica, con la sede Arica de la Universidad del Norte.

AL SEÑOR
ESTEBAN GÁLVEZ ARRIAZA
CONTRALOR REGIONAL (S) DE ARICA Y PARINACOTA
PRESENTE

Luego, a través del decreto N° 674, de 1982, de esa casa de estudios, se oficializó la estructura académica de la UTA, creando seis facultades y dos Institutos, adscribe los departamentos y carreras a cada facultad, dependientes jerárquicamente del Decano de Facultad y señala que entrará en vigor a contar de 1 de marzo de 1983.

Actualmente, la Universidad es una corporación de derecho público, autónoma, con personalidad jurídica y patrimonio propio, que integra el Consejo de Rectores de las Universidades Chilenas, CRUCH.

Ahora bien, en cuanto a la materia objeto de la presente revisión, cabe precisar que la normativa atingente a la fiscalización, se encuentra contenida en el decreto N° 83, de 2004, del Ministerio Secretaria General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado, sobre Seguridad y Confidencialidad de los Documentos Electrónicos, el que en su artículo 1°, establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los Órganos de la Administración del Estado, y las demás, cuya aplicación se recomienda para los mismos fines.

Por medio del oficio N° E486389, de 2024, de esta procedencia, con carácter confidencial, fue puesto en conocimiento de la Universidad de Tarapacá, el preinforme de auditoría N° 68, de 2023, con la finalidad de que formulara los alcances y precisiones que, a su juicio, procediera, lo que se concretó por medio del oficio REC N° 1.214, de 5 de junio de 2024, ingresado a esta Contraloría Regional en esa misma data.

OBJETIVO

La fiscalización tuvo por objeto efectuar una auditoría al Macroproceso de Tecnologías de la Información, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por esa entidad, a través de la existencia y aplicación de políticas, normas y procedimiento de seguridad informática que permitan asegurar la integridad, confiabilidad y confidencialidad de la información en sus sistemas informáticos y redes de comunicación, conforme a las Normas Técnicas aplicables para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, aprobada por el artículo primero del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia.

METODOLOGÍA

El examen se practicó de acuerdo con la metodología de auditoría de este Organismo Superior de Control, y de las disposiciones contenidas en la resolución N° 10, de 2021, que Fija las Normas que Regulan las Auditorías Efectuadas por la Contraloría General de la República, además de los procedimientos de control aprobados mediante resolución exenta N° 1.485, de 1996, que Aprueba Normas de Control Interno de la Contraloría General considerando los resultados de la evaluación de control interno y determinándose la realización de pruebas de auditoría en la medida que se estimaron necesarias.

Las observaciones que la Contraloría General formula con ocasión de las fiscalizaciones que realiza se clasifican en diversas categorías, de acuerdo con su grado de complejidad. En efecto, se entiende por Altamente complejas (AC)/Complejas (C), aquellas observaciones que, de acuerdo con su magnitud, reiteración, detrimento patrimonial, graves debilidades de control interno, eventuales responsabilidades funcionarias, son consideradas de especial relevancia por la Contraloría General; en tanto, se clasifican como Medianamente complejas (MC)/Levemente complejas (LC), aquellas que tienen menor impacto en esos criterios.

UNIVERSO Y MUESTRA

De acuerdo con los antecedentes proporcionados por la entidad fiscalizada, durante el período comprendido entre el 1 de enero y el 31 de diciembre de 2021, el universo de equipos con los que contaba la Universidad de Tarapacá, ascendió a 551 registros.

Las partidas sujetas a examen se determinaron mediante un muestreo por registros, con un nivel de confianza del 90% y un margen de error del 3%, selección que se efectuó de manera estratificada de acuerdo con el tipo de equipo, obteniéndose una muestra de 89 registros, lo que equivale al 16,15% del universo antes indicado, de acuerdo con el detalle que se presenta en la tabla siguiente:

Tabla N° 1: Universo y muestra

Variable	Universo	Muestra	% Examinado
Equipos	551	89	16,15

Fuente: Elaborado a partir del detalle de equipos proporcionado por la universidad.

En este contexto, cabe precisar que la presente auditoría contempló la revisión de la existencia de hardware, usuarios habilitados, de los softwares instalados, con sus respectivas licencias, entre otras materias.

RESULTADO DE LA AUDITORÍA

El resultado de la auditoría practicada se expone a continuación:

I. ASPECTOS DE CONTROL INTERNO

Como cuestión previa, el control interno es un proceso integral y dinámico que se adapta constantemente a los cambios que enfrenta la organización, es efectuado por la alta administración y los funcionarios de la institución, está diseñado para enfrentar los riesgos y para dar una seguridad razonable del logro de la misión y objetivos de la entidad; cumplir con las leyes y regulaciones vigentes; entregar protección a los recursos de la entidad contra pérdidas por mal uso, abuso, mala administración, errores, fraude e irregularidades, así como

también, para la información y documentación, que también corren el riesgo de ser mal utilizados o destruidos.

En este contexto, el estudio de la estructura de control interno de la entidad y de sus factores de riesgo, permitió obtener una comprensión del entorno en que se ejecutan las operaciones relacionadas con la materia auditada, del cual se desprenden las siguientes observaciones:

1. Sistema sin actualizar

De la revisión del sistema de gestión de proyectos desarrollado por la universidad de Tarapacá, para gestionar los datos de las iniciativas del Ministerio de Educación, efectuada el 7 de diciembre de 2022, en compañía de don Jorge Veliz Capetillo, profesional DIPLAN, se advirtió que la información cargada en el sistema data de septiembre de 2022, según consta en acta de fiscalización N° 60 de la misma fecha, por cuanto dicha plataforma está siendo usada como repositorio y aun no se ha puesto en producción para ser usado con el fin específico para el cual fue creado.

Lo anterior, no se ajusta a lo establecido en el artículo 6° sobre información y comunicación, de la citada resolución exenta N° 1.962 de 2022, de este origen, en estable que, las jefaturas de la entidad deben desarrollar e implantar actividades de control sobre la integridad de los datos introducidos en los sistemas de información, así como sobre el procesamiento de dichos datos, para transformarlos en información que pueda ser utilizada por otros controles.

Agregando que, la habilidad de la alta dirección para tomar decisiones apropiadas se ve influenciada por la calidad de la información. La capacidad de generar información de calidad comienza con el análisis de los datos relevantes, por cuanto si se dispone de datos poco precisos o incompletos, la información derivada puede provocar que se adopten decisiones equivocadas, que se efectúen estimaciones erróneas o que se aplique de manera deficiente el criterio profesional de la alta dirección de la entidad.

En respuesta a la observación, la universidad señala que se ha realizado una implementación gradual en el sistema de gestión de proyectos, y que actualmente alberga, 62 proyectos distribuidos en tres fondos, de los cuales aproximadamente 17 son considerados históricos y el resto se encuentran activos.

A lo anterior, añade que a través de la Dirección de Planificación y Proyectos, actualizará la información de los proyectos aprobados y oficializados que corresponden al referido sistema, en un plazo de 60 días hábiles y capacitará a los distintos estamentos universitarios que componen el modelo de gestión en el mencionado sistema, para lo cual, se adjunta un carta Gantt que contiene 3 hitos, la recopilación de antecedentes de los proyectos, capacitaciones a usuarios del sistema de proyectos, y feedback preinforme de auditoría N° 68, de 2023.

Atendiendo que la casa de estudios confirma el alcance formulado, y que las medidas informadas se materializarán en el futuro, se mantiene la observación.

En virtud de lo expuesto, la universidad deberá remitir el respaldo que dé cuenta del cumplimiento de los hitos dispuestos en su carta gantt, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del de Sistema de Seguimiento y Apoyo CGR.

II. EXAMEN DE LA MATERIA AUDITADA

2. Encargado de Seguridad.

De acuerdo con las respuestas otorgadas por la Universidad de Tarapacá a la solicitud de información N° 2, se observa que no existe en esta institución un encargado de seguridad.

Sobre la materia, la inexistencia de un documento que designe a un funcionario competente como oficial de seguridad, imposibilita el desarrollo de políticas de seguridad, asesoramiento a las áreas de la organización que requieran de procedimientos tecnológicos, coordinación de respuesta ante incidentes que afecten a los activos de información institucional, sensibilización de la aludida seguridad a los funcionarios de la repartición, entre otras funciones.

Lo anteriormente descrito vulnera lo establecido en el artículo 4° del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado, sobre Seguridad y Confidencialidad de los Documentos Electrónicos, según el cual los Subsecretarios y Jefes de Servicio deberán designar, dentro del plazo de 30 días contados desde la fecha de total tramitación del decreto enunciado, un Encargado de Seguridad, para que desarrolle e implemente las políticas de seguridad en forma conjunta con el Comité de Gestión de Seguridad y Confidencialidad, y su artículo 12, que las funciones específicas que desempeñe internamente el encargado de seguridad serán establecidas en la resolución que lo designe.

En relación con la presente observación, la Universidad de Tarapacá señala que, mediante decreto exento N° 426, de 3 de junio de 2024, se designó como Encargado de Seguridad, al Director (a) de la Dirección de Gestión Digital y Transparencia de la Universidad de Tarapacá o quien lo subrogue.

En virtud de lo expuesto, considerando que la universidad acreditó la emisión del aludido acto administrativo, se subsana la observación.

3. Gestión de Riesgo.

Se advierte que no existe una periodicidad en el desarrollo de las evaluaciones de riesgo, y que la institución no ha formalizado dicha materia.

Al respecto, este análisis es necesario para el desarrollo del plan de contingencia, así como también para sus pruebas y actualizaciones.

Lo indicado vulnera lo establecido en la letra i) del artículo 37 del referido decreto N° 83, de 2004, que dispone, que se aplicarán las estipulaciones del capítulo 11 de la norma NCh2777, en su integridad, que corresponde al numeral 14 de la Norma Chilena NCh N° 27.002, de 2009.

A mayor abundamiento, el numeral 14.1.2, establece que las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los procesos del negocio.

Añade, que estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, e incluir los resultados específicos para la seguridad de la información, que es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos de continuidad del negocio de la organización y que la evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

De igual modo, indica que, dependiendo de los resultados de la evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez que se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de ésta.

Luego, el numeral 14.1.5 dispone que los planes de continuidad del negocio se deberían someter a pruebas y actualizar regularmente para asegurar su validez y su eficacia.

En su respuesta, la Universidad señala que mantiene implementada una matriz de riesgo de seguridad digital, la cual cuenta con indicadores para determinar el valor del activo de la información y el impacto que este podría provocar en caso de algún tipo de incidente; la que se desarrolla y actualiza con una periodicidad anual, y representa los tipos de amenazas que se puedan presentar.

Agrega, que atendido que la Política de Seguridad será actualizada, en dicho proceso se revisará la mencionada matriz a fin

de que se ajuste a lo establecido en la referida letra i) del artículo 37 del referido decreto N° 83, de 2004.

En virtud de lo expuesto, si bien la casa de estudios informa que la periodicidad del desarrollo y actualización de la matriz es anual, no aporta antecedentes que den cuenta que esta materia se encuentre consignada en algún documento.

A su vez, y considerando que la anotada política será actualizada en el futuro, se resuelve mantener la observación.

Por lo anterior, la Universidad de Tarapacá deberá remitir la Política de Seguridad actualizada, debidamente sancionada por acto administrativo, la que deberá consignar la periodicidad anual que informó en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

4. Política de Seguridad.

Si bien se observa que la Universidad de Tarapacá cuenta con un documento que precisa los procedimientos sobre la Seguridad de la Información, denominado “Política de Seguridad de la información”, aprobado mediante decreto exento N° 187, de 17 de marzo de 2020, se aprecia que este no incluye, dentro del marco donde se fijaron objetivos de control y controles, la estructura de la evaluación del riesgo y su gestión, vulnerando lo detallado en el numeral 5.1.1 de la Norma Técnica NCh-ISO N° 27.002, de 2022, que trata sobre documento de política de seguridad de la información.

Asimismo, se observa que los objetivos planteados en el numeral 3, “Objetivos de la Política y Sistema de Seguridad de la Información”, no son abordados ni desarrollados dentro de referido documento, a modo de ejemplo, cabe precisar que en dicho apartado se consigna como objetivo el “analizar los riesgos que permitan diseñar y establecer medidas que los disminuyan y que estén de acuerdo con la normativa vigente”, y no hay mención del riesgo en algún otro punto del documento.

En sus descargos, la universidad indica que procederá a complementar el aludido decreto exento, en un plazo de 90 días hábiles, y que para su materialización, adjunta el plan de trabajo correspondiente.

Al respecto, considerando que la medida informada se concretará en el futuro, se mantiene la observación.

En virtud de lo expuesto, la Universidad de Tarapacá, deberá remitir la Política de Seguridad actualizada, y debidamente sancionada por medio de acto administrativo, dando cumplimiento a lo establecido en el numeral 5.1.1 de la Norma Técnica NCh-ISO N° 27.002, de 2022, un plazo de 60 días hábiles contados desde la recepción del presente informe, por medio del Sistema de Seguimiento y Apoyo CGR.

5. Comité de Seguridad.

Si bien se advierte que la Universidad de Tarapacá, mediante decreto exento Nº 186, de 17 de marzo de 2020, creó el comité de seguridad de la información estableciendo que este, estaría integrado por el oficial de seguridad de la información, el Encargado de la Unidad de informática y los Directores de Administración y Finanzas, de Planificación y Proyectos, de Gestión de Personas, y de Logística y Operaciones, o a quienes estos designen, de acuerdo a lo señalado por la Universidad de Tarapacá el 9 de septiembre de la presente anualidad, en documento de respuesta a la solicitud de información Nº 2, este no se ha conformado.

Lo anterior impide, entre otros aspectos, emitir lineamientos para la gestión de la seguridad de la información; revisar y aprobar las políticas de seguridad; conocer los riesgos a los cuales se encuentran expuestos los activos de información; revisar y analizar incidentes de seguridad; y aprobar iniciativas para mejorar las operaciones informáticas.

Lo expuesto transgrede la letra b) del artículo 37, del anotado decreto N° 83, de 2004, sobre Seguridad Organizacional, y los numerales 6.1.1 y 6.1.2, de la Norma Técnica NCh-ISO N° 27.002, de 2009, referentes al compromiso de la dirección y coordinación con la seguridad de la información, respectivamente, en el sentido de que el Comité de Seguridad debería estar constituido con líderes o por representantes de la dirección con funciones transversales, de partes importantes de la organización, para coordinar la implementación de los controles de la seguridad de la información y dar cumplimiento a las funciones del Comité señaladas precedentemente.

A mayor abundamiento, entre las funciones del Comité de Seguridad de la Información se encuentra la revisión y aprobación, en forma conjunta con el Encargado de Seguridad, de la política de seguridad de la información y de las responsabilidades generales.

En respuesta a la observación planteada, la universidad señala que el comité originalmente formado sesionó en dos oportunidades durante el mes de mayo del 2024, oportunidad en que se propuso actualizar el acto administrativo que nombra al referido comité de seguridad, definiendo reuniones ordinarias a realizarse periódicamente en el año y reuniones extraordinarias.

Conforme con lo anterior, agrega que procederá a actualizar el decreto exento N° 186, de 2020, de forma tal que, los integrantes del “Comité de Seguridad de la información”, actualicen su integración y cometidos a la estructura y labores que, actualmente se requiere de dicha entidad colegiada.

En virtud de lo expuesto, atendiendo que la universidad acreditó que el comité se conformó y que ha definido las acciones a seguir, se subsana la observación.

6. En cuanto a la validación de equipos

6.a Equipos no encontrados.

Si bien la Universidad posee un inventario de equipamiento, y un reglamento, registro y control de bienes muebles e inmuebles, el cual se encuentra formalizado por decreto exento N° 607, de 2 de septiembre de 2022, constatándose que todo el equipamiento informático se encuentra inventariado y que existe un responsable asignado para cada uno de estos activos, de la revisión de la muestra de equipos, la cual ascendió a 89 computadores, se observó que la mayoría de estos no se encontraban en su ubicación o estaban dentro de la dependencia, pero no se tenía claridad de su ubicación real.

En este contexto, como resultado de dicho procedimiento en terreno, realizado en diversas oportunidades hasta el 29 de noviembre de 2022, se pudo verificar la existencia de 73 equipos, situación que no aconteció con los 16 restantes, cuyo resumen se expone a continuación y la individualización de la ubicación informada por la UTA en el anexo Nº 1:

Tabla N° 2: Detalle de equipos no encontrados

N°	Código Bien	Tipo	N°	Código Bien	Tipo
1	53015969-3	Desktop	9	53071152-2	Notebook
2	53071215-2	Notebook	10	53015945-24	Desktop
3	53015959-1	Desktop	11	53071207-1	Notebook
4	53071274-4	Notebook	12	53071159-1	Notebook
5	53071097-1	Notebook	13	53015951-1	Desktop
6	53016046-10	Desktop	14	53071252-4	Notebook
7	53071215-3	Notebook	15	53071156-1	Notebook
8	53015966-2	Desktop	16	53071156-3	Notebook

Fuente: Elaboración propia en base a equipos no encontrados en terreno.

Lo anterior, demuestra que la Universidad no mantiene un control de la ubicación de los bienes, vulnerando los artículos 5º y 6º del referido decreto exento N° 607, del 2022, los cuales consignan que el jefe de una unidad administrativa o académica, será el custodio de los bienes de su unidad, siendo responsable de supervisar el correcto uso, conservación y cuidado de los bienes a su cargo, así como también supervisar los movimientos de los bienes y evaluar las necesidades de mantenimiento que requieran en cada caso; y que el asistente de activo fijo corresponde a aquellos funcionarios designados por la jefatura de una unidad administrativa o académica, quién tendrá la responsabilidad de informar a la Dirección de Logística, Obras y Operaciones los movimientos de bienes, cambio de custodio, pérdida y cualquier acción que involucre la existencia y mantención de un bien mueble de su unidad.

Además, vulnera lo establecido en el artículo 37 letra c), del decreto N° 83, de 2004, de la Secretaría General de la Presidencia, que se refiere a la Norma Técnica NCh 27.002, capitulo 7.1, cuya norma consigna que

se debería implementar y mantener una adecuada protección sobre los activos de la organización.

En su respuesta, la Universidad de Tarapacá señala que llevó a cabo una revisión en terreno, actualizando los custodios y la ubicación de los 16 equipos, acompañando un anexo que da cuenta de dicha información.

Agrega, que, con el objeto de asegurar una mejor gestión y control de los activos informáticos, la Dirección de Infraestructura y Equipamiento de esa casa de estudios, emitió un instructivo, que establece la obligación de todos los funcionarios de informar trimestralmente sobre los equipos computacionales bajo su custodia.

Asimismo, expone que ha reiterado a las unidades académicas la importancia de dar cumplimiento al Reglamento del Registro y Control de Bienes Muebles, donde se contempla la existencia de un Asistente de Activo Fijo o Administrador de Bienes, quien será el responsable de mantener contacto continuo con la Unidad de Activo Fijo.

En relación con lo anterior, si bien la casa de estudios informa las ubicaciones y responsables de los bienes señalados en la tabla N° 2 y en el anexo N° 1, no se advierte que el anotado instructivo se encuentre aprobado por acto administrativo y no remitió el respaldo que acredite la comunicación efectuada a las unidades académicas.

En virtud de lo expuesto, se mantiene el alcance formulado, debiendo la Universidad remitir el acto administrativo que aprueba el instructivo emitido por la Dirección de Infraestructura y Equipamiento, y el respaldo que dé cuenta de la comunicación realizada a las unidades para el cumplimiento del reglamento indicado en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

6.b En cuanto al control de Inventario.

Sobre la materia, de conformidad a lo señalado por el Encargado de Administración de Bienes, don Ernesto Lee Labarca, a través de acta de fiscalización N° 53, el referido decreto exento Nº 607, de 2022, fue distribuido solo una vez a las jefaturas vía correo electrónico, teniendo como consecuencia que los funcionarios desconozcan los procedimientos establecidos en dicho documento.

Lo anterior, quedó evidenciado al realizarse el chequeo de la muestra de inventario de equipamiento computacional, oportunidad en las que se hicieron consultas a los funcionarios relacionadas con el control de bienes los cuales manifestaban su desconocimiento.

A mayor abundamiento, se constató la salida de equipos de la institución sin autorización, en ubicaciones distintas a las registradas y utilizados por usuarios en diversos lugares, y por profesionales que diferían de los

registros proporcionados por la Universidad, lo que fue ratificado por el aludido Encargado de Administración de bienes en acta de fiscalización N° 54, de 23 de noviembre del 2022, quien manifestó no recibir retroalimentación después de la asignación de un bien.

Al respecto, el artículo 6º del mencionado reglamento, dispone que el asistente de activo fijo corresponde a aquellos funcionarios designados por la jefatura de una unidad administrativa o académica, quién tendrá la responsabilidad de informar a la Dirección de Logística, Obras y Operaciones los movimientos de bienes, cambio de custodio, pérdida y cualquier acción que involucre la existencia y mantención de un bien mueble de su unidad, lo que no se aprecia en la especie.

Asimismo, de lo anterior se desprende que la anotada dirección no está cumpliendo su función según el artículo 8º, del referido reglamento, el que señala que deberá velar por el control de los bienes inmuebles institucionales en uso.

En respuesta a la observación, la Universidad señala que debido a que la retroalimentación y actualización de información por parte de las unidades académicas y administrativas se requiere de forma oportuna, para efectos de mantener actualizado el inventario de equipamientos, se ha considerado como propuesta de mejora, que la Dirección de Infraestructura y Equipamiento, enviará periódicamente el Reglamento a todas las jefaturas, con el fin de asegurar que todos los funcionarios conozcan sus responsabilidades respecto al manejo de bienes.

Además, indica que se hará énfasis sobre la importancia de la retroalimentación trimestral, según lo establecido en el instructivo referido en el punto anterior, para garantizar que la información sobre los movimientos de bienes, cambios de custodio y cualquier otra acción relacionada sea comunicada de manera oportuna.

Sobre la materia, considerando que las medidas informadas se materializarán en el futuro, se mantiene la observación.

En virtud de lo expuesto, la Universidad deberá adoptar las medidas de supervisión y control, que sean necesarias, con el objeto de que se dé cumplimiento a las acciones comprometidas en sus descargos y con ello, a las disposiciones contenidas en el aludido reglamento, ajustándose a las definiciones establecidas en el artículo 5°, de la resolución exenta N° 1.962, de 2022, que Aprueba Normas sobre Control Interno de la CGR.

6.c En relación con las hojas de vida.

Se observó que las hojas de vida o fichas de los bienes revisados no se encuentran actualizadas y alimentadas con información exacta, incumpliendo con ello lo consignado en el artículo 4º del reglamento, según el cual todos los bienes inventariables o con control administrativo dispondrán de una ficha y hoja de vida, que corresponderá al documento donde se registren toda la información del bien desde su ingreso hasta la baja en el patrimonio de la Universidad.

Añade que, en la hoja de vida se procederá a ingresar todos los movimientos, sean traslados, salidas, mantenciones, reparaciones, entre otros.

Lo descrito, además no se aviene a lo establecido en el artículo 6° sobre información y comunicación, de la citada resolución exenta N° 1.962 de 2022, de este origen, que establece que las jefaturas de la entidad deben desarrollar e implantar actividades de control sobre la integridad de los datos introducidos en los sistemas de información, así como sobre el procesamiento de dichos datos, para transformarlos en información que pueda ser utilizada por otros controles.

Agregando que, la habilidad de la alta dirección para tomar decisiones apropiadas se ve influenciada por la calidad de la información. La capacidad de generar información de calidad comienza con el análisis de los datos relevantes, por cuanto si se dispone de datos poco precisos o incompletos, la información derivada puede provocar que se adopten decisiones equivocadas, que se efectúen estimaciones erróneas o que se aplique de manera deficiente el criterio profesional de la alta dirección de la entidad.

En su respuesta, la Universidad manifiesta que las salidas y mantenciones de los bienes se registran en un sistema de gestión de salidas separado, donde se documenta el motivo de la salida, fecha de salida, fecha de regreso, la ubicación temporal y los responsables de cada movimiento y que la ficha de cada bien incluye información crítica como vida útil, depreciaciones y documentos contables.

Añade, que la inclusión de todos los detalles adicionales puede ralentizar el proceso de recuperación en línea, razón por la cual, actualmente las fichas muestran el custodio anterior como un dato histórico, no obstante, es posible recuperar información detallada sobre movimientos históricos de custodios cuando se le instruye al sistema para que refleje estos datos específicos en cada solicitud.

Finalmente, expone que la Dirección de Infraestructura y Equipamiento, propuso como una medida para subsanar el alcance formulado, la implementación de una mejora al sistema de gestión de las hojas de vida, de manera que las fichas reflejen los cambios de ubicación históricos junto con los cambios de custodios de cada bien, permitiendo una mayor transparencia y precisión en el registro de los movimientos de los bienes, facilitando la toma de decisiones basada en información completa y actualizada.

Al respecto, considerando que las medidas informadas se materializarán en el futuro, se mantiene la observación.

En virtud de lo expuesto, la Universidad deberá remitir la documentación que da cuenta de la materialización de la medida indicada precedentemente, en un plazo de 60 días hábiles contados desde la recepción del presente informe, lo que debe ser acreditado en el Sistema de Seguimiento y Apoyo CGR. (C).

6.d Responsable y ubicación de equipos.

Se advirtió que varios equipos se encuentran asignados a un responsable, según área, siendo estos en su mayoría jefes de unidad administrativa o académica, y cuyo resumen se indica en la siguiente tabla, y no al funcionario que manipula u ocupa el equipo computacional para desempeñar sus actividades laborales, lo que concuerda con lo expuesto en el artículo N° 5 del decreto exento N° 607, 2022, pero la asignación por parte del responsable al funcionario correspondiente no se encuentra registrada, perdiendo el control que debe tener la unidad responsable del control de bienes sobre la ubicación y su asignación, lo que tiene como consecuencia las situaciones detectadas durante la revisión de la muestra en terreno.

Tabla N° 3: Dependencias con más de dos equipos

Dependencia	Equipos asignados
Centro de desarrollo de negocios DEVM	4
Oficina Profesionales OTL	3
Oficina Decana	7
Oficina del director	21
Oficina secretaria	3

Fuente: Elaboración propia en base a las validaciones en terreno y a los registros proporcionados por la UTA.

Lo expuesto anteriormente, vulnera lo establecido en el artículo 37 letra c), del decreto N° 83, de 2004, que se refiere a la Norma Técnica NCh 27.002 capitulo 7.1 enfocado al control, y trata el tema de delegación de un activo, manteniendo la responsabilidad.

A mayor abundamiento, útil resulta consignar que el aludido capítulo, sobre responsabilidad de los activos, dispone que su objetivo consiste en implementar y mantener una adecuada protección sobre los activos de la organización; que todos los activos deberían tener un responsable y se debería asignar un dueño a cada uno de ellos; que se deberían identificar los dueños para todos los activos y se debería asignar la responsabilidad del mantenimiento de los controles apropiados; y que la implementación de controles sobre un activo podría ser delegada por su dueño pero éste continúa manteniendo la responsabilidad por la protección del mismo.

Sobre lo observado, la Universidad señala que los equipos están asignados a responsables de áreas, generalmente jefes de unidades administrativas o académicas, de acuerdo con la información proporcionada al momento de la compra, añadiendo que, en diversos casos, estos son los responsables de proyectos y que, conforme al artículo 5° del Reglamento de Registro y Control de Bienes Muebles, actúan como custodios de los bienes en cuestión.

En este contexto, añade que la Dirección de Infraestructura y Equipamiento se compromete reenviar el aludido reglamento a todas las unidades, hacer énfasis en la retroalimentación continua que debe existir para mantener informada a la aludida dirección, en la sensibilización, monitoreo, y

capacitaciones necesarias para mejorar el control y la protección de los activos de la universidad, asegurando el cumplimiento de las normativas vigentes y facilitando la gestión eficiente de los recursos.

Al respecto, atendiendo que las medidas informadas se materializarán en el futuro, se mantiene la observación.

En virtud de lo expuesto, la Universidad deberá remitir el inventario de equipos con el detalle de los responsables, ubicación y funcionario que se encuentra utilizando dichos bienes, en un plazo de 60 días hábiles contados desde la recepción del presente informe, lo que debe ser acreditado en el Sistema de Seguimiento y Apoyo CGR.

Asimismo, deberá adoptar las medidas de supervisión y control, que sean necesarias, con el objeto de que se dé cumplimiento a las acciones comprometidas en sus descargos, ajustándose a las definiciones establecidas en el artículo 5°, de la resolución exenta N° 1.962, de 2022, que Aprueba Normas sobre Control Interno de la CGR.

7. Activos sin registro de custodio en información entregada.

Realizado el análisis del inventario de 551 equipos declarados por la Universidad se advirtió la existencia de 123 equipos sin custodio, según se puede apreciar detalle en anexo N° 2.

Lo indicado precedentemente, incumple lo señalado en el artículo 37 letra c), del decreto N° 83, de 2004, que se refiere a la Norma Técnica NCh 27.002 capitulo 7.1 enfocado al control, y trata el tema de delegación de un activo, manteniendo la responsabilidad.

A mayor abundamiento, útil resulta consignar que el aludido capítulo, sobre responsabilidad de los activos, dispone que su objetivo consiste en implementar y mantener una adecuada protección sobre los activos de la organización; que todos los activos deberían tener un responsable y se debería asignar un dueño a cada uno de ellos; que se deberían identificar los dueños para todos los activos y se debería asignar la responsabilidad del mantenimiento de los controles apropiados; y que la implementación de controles sobre un activo podría ser delegada por su dueño pero éste continúa manteniendo la responsabilidad por la protección del mismo.

En relación con la materia, la Universidad indica que los bienes indicados en el citado anexo sí mantendrían su ubicación y responsable actualizado en el sistema, adjuntando como respaldo una tabla con el detalle de dicha información.

A lo anterior, añade que, para efectos de mejorar la gestión y asegurar una retroalimentación más efectiva, se realizó funcionalidad en el sistema de control de bienes, la que solicitará el visto bueno de aceptación de asignación de bienes a cada custodio, especialmente para compras nuevas.

Continúa exponiendo, que se generará un acta digital de aceptación para todos los funcionarios de la Universidad a quienes se les asignen bienes computacionales, documento obligatorio que cada custodio debe firmar electrónicamente, confirmando la recepción y responsabilidad del equipo asignado.

En virtud de lo expuesto, considerando que la universidad informó el detalle de las ubicaciones y custodios de los bienes, y las medidas para evitar la reiteración de las situaciones advertidas, se subsana la observación.

8. Respecto a la Sala de Servidores

Como resultado de las validaciones efectuadas a la seguridad física de la plataforma de tecnologías de información que mantiene la Universidad de Tarapacá de Arica, y lo confirmado por don Oscar Sagardia Osorio, Encargado del Área de Informática, según consta en el formulario de plan de pruebas de sala de servidores, de 25 de octubre de 2022, se constataron las siguientes situaciones:

8.a Seguridad Física de la Plataforma

i) La sala de servidores no cuenta con alarma en acceso o puerta.

ii) No existen señaléticas adecuadas en las salidas de emergencia en el perímetro cercano a la sala de servidores, estableciendo las rutas de evacuación.

iii) No existe señalética que indique prohibición para fumar, consumir alimentos y bebidas.

iv) No se prohíbe el uso de medios de grabación.

v) No se cuenta con carteles que indiquen prohibición de uso de medios de grabación.

vi) La sala de servidores no cuenta con iluminaria adecuada en caso de corte o falla estas, deben usar aparatos externos para iluminar, como linternas o celulares.

Las situaciones mencionadas sobre la seguridad física de la plataforma, vulneran lo establecido la letra e) del artículo 37 del referido decreto N° 83, de 2004, de la Secretaria General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado Sobre Seguridad y Confidencialidad de los Documentos Electrónicos, que dispone, en síntesis, que para el nivel avanzado de seguridad y del ambiente se aplicarán los numerales 9.1 y 9.2 de la Norma Chilena NCh N° 27.002, de 2009.

A mayor abundamiento, cabe precisar que el numeral 9.1.1, dispone que se deberían utilizar perímetros de seguridad para proteger las áreas que contienen información e instalaciones de procesamiento de información; 9.1.5, se debería diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras; 9.2.1, el equipamiento se debería ubicar o proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado; y 9.2.2, se debería proteger el equipamiento contra posibles fallas en el suministro de energía y otras interrupciones causados por fallas en elementos de soporte.

Sobre las observaciones planteadas, la casa de estudios superiores informó que levantó el proceso de adquisición de un control de acceso para la puerta de la sala de servidores, a través de mercado público; que entregó los registros fotográficos con la señalética de salida de emergencia, de prohibición para fumar, consumir alimentos y bebidas, del uso de medios de grabación, y que se efectuó la solicitud para instalar iluminación en el data center.

En virtud de lo señalado, se subsana lo objetado.

8.b Controles Ambientales

i) En caso de emergencia se cuenta con equipos de aire acondicionado, siendo estos los que funcionan en la actualidad y los principales se encuentran desconectados por remodelación.

8.c Suministro de Energía

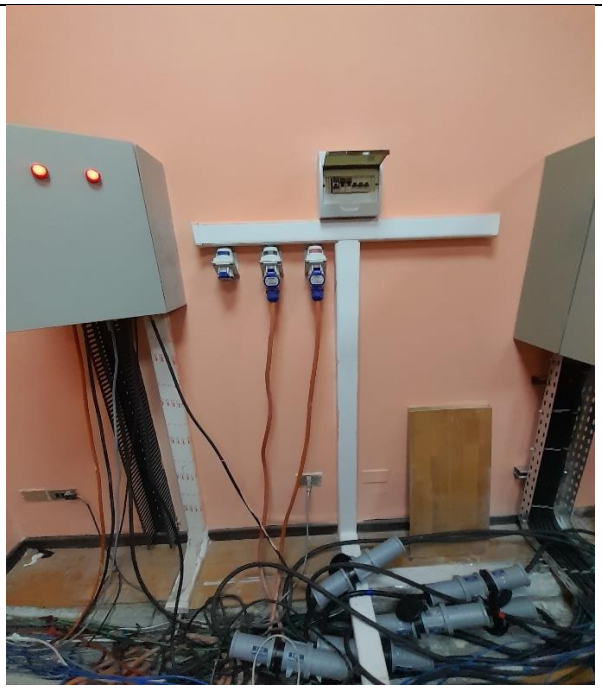
i) Los cables de suministro de energía no se encuentran protegidos ya que varios de los equipos están conectados con alargadores en forma desordenada, por motivos de remodelación, tal como se expone a continuación:

Tabla N° 4: Detalle de deficiencia detectada

Cables de suministro de energía

ii) No cuentan con rotulación adecuada en los interruptores de energía, lo cual se visualiza en la siguiente imagen:

Tabla N° 5: Fotografías de interruptores



Interruptores mencionados

Las situaciones descritas en los numerales 8.b y 8.c, relacionadas con los controles ambientales y el suministro de energía, vulneran lo establecido la letra e) del artículo 37 del referido decreto N° 83, de 2004, de la Secretaria General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado Sobre Seguridad y Confidencialidad de los Documentos Electrónicos, que dispone, en síntesis, que para el nivel avanzado de seguridad y del ambiente se aplicarán los numerales 9.1 y 9.2 de la Norma Chilena NCh N° 27.002, de 2009.

A mayor abundamiento, el numeral 9.2.1, señala que el equipamiento se debería ubicar o proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, detallando en su letra f), que las condiciones ambientales, tales como temperatura y humedad, se deberían supervisar para verificar que las mismas no afectan negativamente el funcionamiento de las instalaciones de procesamiento de la información, y oportunidades de acceso no autorizado; y 9.2.2, que se debería proteger el equipamiento contra posibles fallas en el suministro de energía y otras interrupciones causados por fallas en elementos de soporte.

En cuanto a lo consignado en el numeral 8.b, la Universidad informa que los sistemas de aire acondicionado se encuentran habilitados, tanto el principal, como los sistemas secundarios, adjuntando como

respaldo imágenes e información de la temperatura de la sala de servidores, por lo que se subsana el alcance formulado.

Por otra parte, en relación con lo señalado en el numeral 8.c, la Universidad manifiesta que, en el momento en que se realizó la fiscalización las instalaciones se encontraban en un periodo de cambios estructurales y mejoras, y que en la data de emisión de su respuesta los cambios ya se encuentran realizados, y adjunta una imagen que da cuenta del estado actual de la sala de servidores, la que da cuenta de la regularización de lo observado.

Ahora bien, considerando que la Universidad acredita que los cables de suministro de energía se encuentran protegidos y ordenados, se subsana lo consignado en el literal i), del numeral 8.c, sin embargo, atendido que en la imagen acompañada no se visualiza la rotulación adecuada en los interruptores de energía, por lo que el alcance formulado en el literal ii, se mantiene.

En virtud de lo expuesto, la Universidad deberá remitir el respaldo fotográfico que respalde la rotulación indicada, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

8.d Compra y Mantención de Arquitectura Tecnológica

i) No posee una bitácora de fallas detectadas de los equipos de la sala de servidores.

ii) No existe un proceso o servicio de mantenimiento para todos los equipos de la sala de servidores.

Al respecto, lo indicado precedentemente, vulnera lo dispuesto en la letra e) del artículo 37 del referido decreto N° 83, de 2004, de la Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado Sobre Seguridad y Confidencialidad de los Documentos Electrónicos, que dispone, en síntesis, que para el nivel avanzado de seguridad y del ambiente se aplicarán los numerales 9.1 y 9.2 de la Norma Chilena NCh N° 27.002, de 2009.

En este contexto, el numeral 9.2.4, señala que el equipamiento se debería mantener adecuadamente para asegurar su continua disponibilidad e integridad.

En respuesta, la Universidad informa que, como parte de la mejora continua de la institución y proceso de transformación digital, se implementó un sistema de registro de incidentes, y que, en cuanto al servicio o proceso de mantenimiento, este se ha estado realizando desde el año 2022, según dan cuenta los respaldos contenidos en las imágenes que acompaña.

Al respecto, considerando que la casa de estudios acredita las medidas implementadas y las acciones ejecutadas en relación

con el mantenimiento de los servidores, se subsanan las observaciones contenidas en el presente numeral.

9. Procedimiento de destrucción de información.

De acuerdo con lo informado por la Universidad de Tarapacá el 9 de septiembre de 2022, en documento de respuesta a la solicitud de información Nº 2, se observa que dicha institución no cuenta con un procedimiento de destrucción de información.

Lo anteriormente expresado, no se ajusta a lo establecido en la letra f) del artículo 37 del decreto N° 83, de 2004, sobre Gestión de Operaciones y Comunicaciones, y el numeral 10.7 de la Norma Técnica NCh-ISO N° 27.002, de 2009, referentes al manejo de medios, el que establece como su objetivo evitar divulgación no autorizada, modificación, borrado o destrucción de los activos, interrupción de las actividades del negocio y señala que se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra daño, borrado y acceso no autorizado.

En su respuesta, la Universidad señala que, mediante un plan de trabajo, procederá a actualizar su política de seguridad incorporando una política de destrucción de información de acuerdo con las disposiciones legales y técnicas previamente señaladas.

En virtud de lo expuesto, atendiendo que las medidas informadas se materializarán en el futuro, se mantiene la observación.

Por lo anterior, la Universidad deberá remitir la política de destrucción de información, debidamente sancionada por acto administrativo, en un plazo de 60 días hábiles contados desde la recepción del presente informe, lo que debe ser acreditado en el Sistema de Seguimiento y Apoyo CGR.

10. Sociabilización de la política.

Si bien se advirtió la existencia de un instructivo sobre uso de software legal, aprobado mediante decreto exento Nº 614, de 2012, de conformidad a lo señalado por don Oscar Sagardia Osorio, Encargado de la Unidad de Desarrollo Tecnológico de la universidad, en adelante UDT, mediante acta de fiscalización N° 48, de 26 de octubre de 2022, esta no se sociabiliza, ya sea por correo electrónico, intranet, banner y capacitaciones, entre otros, lo que vulnera lo establecido en el artículo 22 del referido decreto N° 83, de 2004, que enfatiza que, en todos los organismos sujetos a esa norma, deberán explicitarse y difundirse aspectos como; contactos de apoyo; cumplimiento en licencia de software y su uso; buenas prácticas para protección del riesgo asociados a la obtención de archivos y software a través de las redes de telecomunicaciones, o por otros medios.

En su respuesta, la Universidad manifiesta que la Dirección de Gestión Digital y Transparencia, procederá a sociabilizar de forma

regular el instructivo sobre uso de software legal a través de la intranet, y boletín institucional de manera periódica, disponiéndose aquello mediante una instrucción y acampanándose el requerimiento de trabajo para ese efecto.

Como complemento a lo anterior, expone que se propone desarrollar capsulas informativas relacionadas con las diversas políticas de seguridad de la información y también desarrollar una aplicación donde se valide parte de los usuarios el conocimiento de mencionado instructivo.

Al respecto, atendiendo que las medidas informadas se materializarán en el futuro, se mantiene la observación.

En virtud de lo expuesto, la Universidad deberá remitir los antecedentes que acrediten la implementación de las medidas informadas en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, lo que debe ser acreditado en el Sistema de Seguimiento y Apoyo CGR.

11. Rol de administrador en perfiles de usuario.

De las validaciones efectuadas en terreno a los equipos estacionarios y portátiles, se advirtieron diversas deficiencias en cuanto a los controles, las cuales se detallan a continuación:

a) Cuentas locales con permiso de administración.

b) Cuentas locales sin claves.

c) No existe una cuenta destinada exclusivamente a la administración, considérese como administración de equipos al personal encargado de instalación y desinstalación de programas, configuraciones personalizadas de IP, configuraciones avanzadas, etc.

d) Las cuentas de usuario no tienen nombres que identifiquen a los usuarios o con nombres estandarizados.

e) Cualquiera puede instalar un software y cualquiera tiene acceso.

f) No existen controles.

Lo anterior, incumple lo establecido en el decreto N° 83 en su letra f) del artículo 37, referente a la gestión de las operaciones y comunicaciones y de acuerdo con lo dispuesto en la norma NCHS 27.002, numeral 10.10.2, sobre supervisión y uso de sistemas.

A mayor abundamiento, es del caso señalar que el anotado apartado dispone que se deberían establecer procedimientos para supervisar el empleo de instalaciones de procesamiento de la información y revisar con regularidad los resultados de las actividades de supervisión, añadiendo que es

necesario utilizar procedimientos de supervisión para asegurar que los usuarios sólo realizan las actividades que explícitamente se les han autorizado.

Enseguida, el numeral 10.4.1 dispone que se deberían implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto a procedimientos adecuados para concientizar a los usuarios y que la protección contra el código malicioso se debería basar en el empleo de sistemas de detección y reparación, en la conciencia de la seguridad, y en apropiados controles de acceso al sistema y gestión de cambios.

Asimismo, se aprecia una vulneración a lo establecido por la universidad en la Política de General de Seguridad de la Información de la Universidad de Tarapacá, según decreto exento 187, de 2022, específicamente en el punto 2 sobre "Políticas de Control de acceso a la información", además de lo consignado en el artículo 20, del anotado decreto N° 83, de 2004, permitiendo a los usuarios instalar y desinstalar indiscriminadamente cualquier aplicación, ya que no existe ningún mecanismo de control para evitar este proceder, con respecto a mantener los equipos con cuentas con permiso de administrador.

En sus descargos, respecto de lo establecido en la letra a), la Universidad informó que ha iniciado un proceso de revisión y ajuste de los permisos de las cuentas locales, de forma tal que, solo el personal autorizado tenga privilegios administrativos y que implementará una disposición que prohíba permisos administrativos en cuentas no autorizadas.

A su vez, en relación con el literal b), señala que procederá a implementar una disposición que requiere contraseñas robustas para todas las cuentas locales, sin perjuicio de informar, que se ha configurado el sistema para que obligue a la creación de contraseñas al configurar nuevas cuentas.

Por su parte, en cuanto al literal c), la Universidad detalla que ha procedido a iniciar la creación de cuentas específicas para tareas administrativas, destinadas únicamente al personal autorizado para la administración de equipos.

Enseguida, en lo que atañe a la letra d), la casa de estudios indica que procederá a implementar una disposición sobre nomenclatura estandarizada para todas las cuentas de usuario que facilite la identificación y el control de acceso, lo que incluirá un formato específico que incorpore elementos identificativos, como el nombre y el departamento del usuario.

A su vez, respecto del literal e), la UTA indica que se procederá a establecer controles críticos para la instalación de software, por lo que, solo el personal con cuentas administrativas especificas tendrá la capacidad de instalar y desinstalar software, y se implementarán soluciones de gestión de aplicaciones que controlen y supervisen la instalación de software.

Finalmente, en cuanto a la letra f), la universidad informa que procederá a desarrollar e implementar un marco integral de controles internos de TI, lo que incluye políticas de seguridad, auditorias regulares de

cuentas y permisos, y la implementación de herramientas de monitoreo y gestión de sistemas para asegurar el cumplimiento de estas políticas.

En virtud de lo expuesto, atendiendo que las medidas informadas por la Universidad se materializarán en el futuro, se mantienen las observaciones.

Por lo anterior, la casa de estudios superiores deberá remitir la documentación de respaldo que acredite la implementación de las medidas informadas en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

12. En cuanto al control de acceso a los equipos

Al respecto, producto del chequeo de la muestra de equipos, se advierte que no existe un sistema que permita tener un control de acceso a los equipos computacionales, ya que estos funcionan mediante cuentas locales, sin ningún tipo de control, muchos con nombre de usuario genérico, otros pocos con clave de acceso local, pero en su mayoría sin contraseña, lo que permite que cualquiera pueda acceder al equipo y a la información disponible en ellos, según consta en acta de fiscalización N° 50, de 26 de noviembre de 2022, firmada por el Encargado de UDT.

Esta falta de control vulnera lo establecido en la letra g), del artículo 37, decreto N° 83, de 2004, que trata sobre el control de acceso, según lo dispuesto en el capítulo 11.1, de la norma chilena N° 27.002.

A mayor abundamiento, el anotado numeral consigna que se debería establecer, documentar y revisar una política de control de acceso, basada en requisitos del negocio y seguridad para el acceso.

Añade, que las reglas de control de acceso y derechos para cada usuario o grupo de usuarios deberían estar claramente establecidas en una política de control de acceso. Los controles de acceso son tanto lógicos como físicos, y éstos se deberían considerar en forma conjunta. Los usuarios y los proveedores de servicio deberían ser provistos de una declaración clara de los requisitos del negocio que deberían cumplir para los controles de acceso.

En su respuesta, la Universidad señala que se realizará la actualización de la política de control de acceso a la información, la cual consideraría medidas asociadas la eliminación de cuentas locales genéricas y creación de cuentas de usuario individualizadas con nombres estandarizados; la implementación de políticas de contraseñas complejas, que incluyan longitud mínima y combinación de caracteres especiales, números y letras; requerimiento de cambio de contraseña periódicamente; la realización de auditorías regulares para verificar el cumplimiento de las políticas de acceso; implementación de herramientas de monitoreo que registren intentos de acceso y actividades de los usuarios; programas de capacitación para usuarios sobre la importancia de la seguridad de la información y las mejores prácticas en el uso de equipos computacionales; e instrucciones sobre creación y mantenimiento de contraseñas seguras y la importancia de cerrar sesión.

Estas acciones establecerán un control de acceso riguroso y efectivo, protegiendo los equipos y la información contenida, garantizando un entorno seguro y confiable para todos los usuarios.

Al respecto, atendiendo que las medidas informadas por la Universidad se materializarán en el futuro, se mantiene la observación.

En virtud de lo expuesto, la casa de estudios deberá remitir la política de control de acceso a la información actualizada, y debidamente sancionada por acto administrativo, en los términos indicados en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

13. Integridad de Respaldos.

De conformidad a las indagaciones efectuadas se determinó que no existe un proceso que regularmente pruebe la fidelidad o integridad de el o los respaldos, ni tampoco es realizado con este objetivo, por cuanto, de acuerdo a lo señalado por don Juan Estonivich Muñoz, Ingeniero de Sistemas de la Universidad de Tarapacá, mediante acta de fiscalización del 26 de octubre de 2022, las pruebas de integridad son hechas bajo demanda de recuperación de información, por ende si el respaldo esta corrupto imposibilita la recuperación de información.

Sobre la materia, el artículo 24 del aludido decreto N° 83, de 2004, consigna que, en los órganos regidos por esa norma, deberán realizarse copias de respaldo de la información y las aplicaciones críticas para la misión de la institución en forma periódica, en conformidad a las reglas que allí se indican.

A mayor abundamiento, la letra c), del anotado artículo, establece que deberá garantizarse la disponibilidad de infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o la falla de un dispositivo. Las configuraciones de respaldo para los sistemas individuales deberán ser probadas con regularidad, a lo menos cada 2 años, para asegurar que ellas satisfacen los requisitos estipulados en los planes de continuidad institucionales.

En su respuesta, la Universidad expone que actualmente se cuenta con una herramienta de respaldo de la información de los servidores y que se agregará una prueba de la fidelidad o integridad de el o los respaldos que se realicen.

Añade, que, como parte de la mejora continua de la institución y proceso de transformación digital, se propone oficializar, como parte de la política de seguridad un procedimiento de respaldo de la información de servidores donde se defina un protocolo de verificación de respaldos.

Al respecto, atendiendo que las medidas informadas se materializarán en el futuro, se mantiene la observación.

En virtud de lo expuesto, la Universidad deberá remitir el procedimiento de respaldo de información que señala en su respuesta, debidamente sancionado por la autoridad, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

14. Política de Control de Acceso.

En relación con las validaciones efectuadas sobre la existencia de un procedimiento formal, se constató que la Universidad de Tarapacá cuenta con una política general de seguridad de la información según decreto exento Nº 187, de 2020, el que trata en su anexo Nº 2 sobre Política de control de acceso a la información, 18 puntos referidos al tema distribuidos en 2 hojas.

En este contexto, como recomendación se sugiere profundizar este ámbito, dando como resultado un documento para permita tener directrices más detalladas, y así llevar un proceso formal para la creación, modificación y eliminación de cuentas de usuario en forma generalizada y estandarizada, para ser usada por los diferentes sistemas, accesos a la red, sistemas operativos.

Sobre la materia, el numeral 11, de la anotada Norma Chilena NCH-ISO Nº 27.002, dispone sobre el control de acceso, que su objetivo consiste en controlar el acceso a la información, que los accesos a la información, a las instalaciones de procesamiento de la información y a procesos del negocio deberían ser controlados sobre la base de requisitos del negocio y seguridad y que las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

Luego, su numeral 11.1.1, consigna que se debería establecer, documentar y revisar una política de control de acceso, basada en requisitos del negocio y seguridad para el acceso.

Añade, que las reglas de control de acceso y derechos para cada usuario o grupo de usuarios deberían estar claramente establecidas en una política de control de acceso. Los controles de acceso son tanto lógicos como físicos, y éstos se deberían considerar en forma conjunta. Los usuarios y los proveedores de servicio deberían ser provistos de una declaración clara de los requisitos del negocio que deberían cumplir para los controles de acceso.

En su respuesta, la Universidad informa que adjunta el plan de trabajo para la actualización y complementación de la Política de control de acceso a la información, en el marco de la “Política general de seguridad de la información”.

Al respecto, considerando que la medida informada se materializará en el futuro, se mantiene la observación.

En virtud de lo expuesto, la Universidad deberá remitir la política de control de acceso actualizada y debidamente sancionada por acto administrativo, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

15. Política interna de Control de Acceso.

Respecto de la política general de seguridad de la información según decreto exento Nº 187, de 2020, de 17 de marzo del 2020, el que trata en el numeral 2, del anexo Nº 1, sobre Política de control de acceso a la información, a continuación, se exponen las vulneraciones detectadas en terreno, las que dicen relación con las cuentas de inicio de sesión de equipos computacionales.

a) Cualquier persona puede tener acceso a la información de los equipos computacionales pertenecientes a la universidad, incluido terceros, ya que no tienen contraseña de acceso, lo que vulnera lo expuesto en el numeral 2.1, “política de Control de Acceso.

A mayor abundamiento, el anotado apartado dispone que todo funcionario perteneciente a la Universidad de Tarapacá, incluidos terceros, deberán tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la organización. El otorgamiento de privilegios y acceso a los activos de información deber están basados en las necesidades de las áreas y aprobadas por los propietarios o custodios de los activos.

b) Se advirtió que los equipos tienen usuarios genéricos y libres de acceso, lo que no se ajusta al numeral 2.2, del referido documento.

Al respecto, el señalado apartado dispone que las necesidades de acceso deberán ser determinadas por las respectivas jefaturas, en función de las tareas asignadas al cargo del funcionario.

c) Asimismo, se observó que no existe un mecanismo, sistema o método de control que permita restringir o permitir el acceso a los equipos computacionales, lo que vulnera lo expuesto en la política de seguridad de la información en su numeral 2.3, del anexo Nº 1, el cual consigna que para todo medio de procesamiento de información al que se necesite conceder accesos (Bases de datos y aplicaciones), el propietario de la información en conjunto con el Área de Desarrollo Tecnológico de la Unidad de Desarrollo Tecnológico (U.D.T.), designará un responsable quien concederá los permisos de acceso respectivos.

d) No existen accesos especiales para terceros, lo que no se aviene a lo expuesto en el numeral 2.4, el cual señala que los accesos a terceros deberán realizarse mediante un acuerdo firmado, con periodo de uso con fecha de expiración y tomando compromiso respecto de la confidencialidad de los datos y accesos concedidos.

A mayor abundamiento, su apartado 2.1 dispone que todo funcionario perteneciente a la Universidad de Tarapacá (U.T.A.),

incluidos terceros, deberán tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la organización. El otorgamiento de privilegios y acceso a los activos de información deber están basados en las necesidades de las áreas y aprobadas por los propietarios o custodios de los activos.

e) La UDT no cuenta con medios de control para suspender la cuenta de un equipo o usuario en específico, ya que son locales, genéricas, de uso libre y perfectamente pueden ser usadas por cualquiera, ya que no son individualizadas, lo que vulnera lo expuesto en la política de seguridad de la información en su numeral 2.5, de la política de Control de Acceso.

En este contexto, dicho apartado dispone que la Unidad de Desarrollo Tecnológico estará siempre facultada para suspender cualquier acceso concedido frente a cualquier sospecha de uso sospechoso o riesgo de pérdida de confidencialidad, integridad o disponibilidad de la información.

f) Si bien la anotada política considera que cualquier intento de acceso no autorizado es considerado un incidente grave, si visualmente funcionarios o personal de seguridad no ven que alguien accede a un computador, jamás será reportado y como institución no podrán tomar medidas, ya que no existe un control de acceso a la información de los equipos, lo que vulnera lo expuesto en el numeral 2.6, el cual añade que dicha materia será reportada y se tomarán las acciones respectivas.

g) No existe la administración de perfiles de usuario, tampoco un administrador de sistema, como comúnmente se le conoce “administrador de dominio”, lo que vulnera lo expuesto en la política de seguridad de la información en el numeral 2.7, según el cual la administración de perfiles de usuario en las aplicaciones será responsabilidad de los usuarios administradores de cada aplicación y las unidades correspondientes.

h) No existe ningún control de acceso para los funcionarios que no hayan completado el proceso de autorización, ya que la cuenta del PC es genérica y sin clave, lo que vulnera lo expuesto en el numeral 2.8, de la Política de Control de Acceso.

i) No existen perfiles de acceso orientados a grupos de usuarios, lo que vulnera lo expuesto en el numeral 2.9.

Al respecto, cabe precisar que el referido apartado dispone que, para facilitar la administración de los accesos, se definirán perfiles de acceso asignables a grupos de usuarios que, por sus responsabilidades en la organización, presenten necesidades de acceso equivalentes.

j) Atendido que la UTA no tiene un sistema que controle el acceso, se desprende que la UDT no ha dado cumplimiento a lo dispuesto en el numeral 2.10, de la política de Control de Acceso, el que establece que la Unidad de Desarrollo Tecnológico implementara las reglas de control de acceso solicitadas por los administradores de aplicación y las unidades correspondientes.

k) No existen perfiles con derecho de acceso individualizados de forma que las acciones realizadas sean de responsabilidad directa del funcionario, lo que vulnera lo expuesto en el numeral 2.12, de la Política de Control de Acceso.

l) Todo perfil local creado en cada equipo o usado por defecto tiene permiso de administración, por lo cual dispone del control total del proceso de negocio en el equipo y a voluntad propia, lo que vulnera lo expuesto en el numeral 2.13, según el cual el otorgamiento de accesos respecto a recursos de información deberá considerar sólo la etapa en la que interviene el funcionario, de modo de que un mismo funcionario (no administrador) pueda disponer por voluntad propia, del control total de un proceso de negocio.

m) No existe un control de acceso lógico, por lo que, ante cambio de funciones, destitución u otro, el funcionario podrá acceder de igual forma a cualquier equipo, lo que vulnera lo expuesto en los numerales 2.16 y 2.17, de la Política de Control de Acceso.

En este contexto, es dable manifestar que los referidos numerales establecen que la Unidad de Recursos Humanos deberá ser responsable de abordar situaciones de cambio de cargo de funcionarios, y dar aviso para revisar permisos de acceso lógico asignados y verificar que éstos sigan siendo válidos de acuerdo a su nueva función; y que la unidad de Recursos Humanos, deberá informar cuando un funcionario cesa su relación laboral con la Universidad de Tarapacá, de manera que todos los permisos y accesos deberán ser revocados. En el caso que otro funcionario ocupe su lugar, deberá crearse los accesos correspondientes con identidad nueva y a partir de la fecha en que asume el nuevo rol, respectivamente.

n) No existe un administrador de cuentas de usuario que permita revisar en forma periódica los perfiles de los usuarios vigentes, así como tampoco un control de los privilegios de los accesos, vulnerando con ello lo expuesto en el numeral 2.18.

A mayor abundamiento, el referido apartado establece que los usuarios administradores de aplicaciones deberán revisar en forma periódica los perfiles de usuarios vigentes y solicitar a la UDT, cualquier cambio que sea necesario para la realización correcta de sus labores; ya se ampliando o reduciendo el límite de sus privilegios en los respectivos sistemas.

En respuesta a lo indicado en los literales a), b), c), d), h), i), k) y l), la Universidad señala que implementará la disposición de creación de cuentas de usuario con contraseñas complejas, que incluyan longitud mínima y combinación de caracteres especiales, números y letras, además del requerimiento de cambio de contraseñas en forma periódica, se procederá a la eliminación de cuentas locales genéricas, y en su reemplazo, se crearán cuentas individualizadas con nombres estandarizados, y accesos especiales a terceros.

Enseguida, en relación con los literales e) y f), informa que se implementarán mecanismos de control que permitan accionar a la UDT

en los términos previamente referidos, conforme a las políticas de control de acceso que se actualizarán.

Luego, en cuanto a la letra g), la Universidad señala que, en el marco de la actualización de la política de control de acceso a la información, se procederá, igualmente, a abordar la presente observación, de manera tal, que se designe y formalice un “administrador de dominio”, mediante acto administrativo de esa casa de estudios.

A su vez, respecto de la letra j), manifiesta que, conforme a los procesos de actualización y complementación de políticas comprometidas en la presente respuesta, se dispondrán los controles de acceso correspondientes, instruyéndose a la UDT, que proceda a dar cumplimiento estricto a los controles que debe observar con ocasión de los procesos que son de su competencia.

Finalmente, en lo que atañe a los literales m) y n), indica que estas observaciones se abordaron previamente, refiriendo que, junto con la actualización y complementación de la política institucional sobre la materia, se procederá a implementar el control de acceso lógico ante cambio de funciones, destitución u otra variación que pueda experimentar la relación de un funcionario en la institución, y a actualizar al administrador de cuentas para usuario.

Al respecto, considerando que las medidas expuestas en los descargos se materializarán en el futuro, se mantienen las observaciones individualizadas precedentemente.

Por tal motivo, en cuanto a las letras a), b), c), d), h), i) y k), la Universidad deberá remitir la documentación de respaldo que acredite la implementación de las medidas informadas en su respuesta.

Luego, en cuanto a las letras e) y f), dicha casa de estudios deberá remitir el detalle de los mecanismos de control implementados, junto con los antecedentes que lo acrediten.

Enseguida, en relación con el literal g), la Universidad deberá remitir la política de control de acceso de la información, que abarque la materia de la presente observación, y el acto administrativo que designe al “administrador de dominio

A su vez, en cuanto a la letra j), la Universidad deberá remitir el detalle de los controles respectivos, junto con su documentación de respaldo.

Finalmente, en lo que atañe a las letras m) y n), la Universidad deberá remitir la política debidamente sancionada por la autoridad, y la documentación que acredite la implementación del control de acceso lógico ante cambio de funciones, destitución u otra variación que pueda experimentar la relación de un funcionario en la institución, y de la actualización del administrador de cuentas para usuario.

Todo lo anterior, deberá ser acreditado, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

16. Estructura de Contraseñas.

Respecto al acceso a los equipos computacionales que permiten a su vez ingresar a la red institucional de la Universidad de Tarapacá y a la documentación en ellos existente, se constató que no existe un sistema centralizado de administración de usuarios que permita a estos dar un identificador único de acceso a cada usuario, lo que tiene como consecuencia tener un proceso de administración de cuentas deficiente o inexistente, el que se realiza mediante cuentas de usuario locales, en cada equipo institucional, los que pueden ser ocupados por cualquier funcionario, ya que están con libre acceso, lo que fue corroborado por don Oscar Sagardia Osorio, Encargado de UDT, a través de acta de fiscalización N° 50, de 26 de noviembre de 2022.

El no tener un identificador para cada funcionario que acceda a la red mediante un dispositivo o estación de trabajo vulnera lo dispuesto en el artículo 32, del decreto Nº 83, de 2004, que trata sobre cómo se deberá controlar el acceso a los servicios de red internos y externos mediante el uso de identificadores o certificados digitales.

En su respuesta, la Universidad indica que, conforme a lo indicado para el numeral anterior, se implementará la disposición de contraseñes complejas, que incluyan longitud mínima y combinación de caracteres especiales, números y letras, además del requerimiento de cambio de contraseñas en forma periódica, de manera tal que se dé cumplimiento a la normativa vigente, se eliminarán las cuentas locales genéricas y, en su reemplazo, se procederá a la creación de cuentas de usuarios individualizadas con nombres estandarizados y accesos especiales a terceros.

Considerando que las medidas informadas se materializarán en el futuro, se mantiene la observación.

Por tal motivo, la Universidad deberá remitir la documentación de respaldo que acredite la implementación de las medidas informadas en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, lo que debe ser acreditado en el Sistema de Seguimiento y Apoyo CGR.

17. Usuarios desvinculados activos en sistema.

Revisados los usuarios que se encuentran perfilados en los diferentes sistemas informáticos administrados por la entidad, se cotejaron cuentas activas de personas que ya no cumplen labores en la Universidad de Tarapacá.

Tabla N° 6: Usuarios no activos en Sistemas Área Administrativa y Financiera

ID Usuario	Nombre	Área	Escalafón
07425042-4	Ángel Suarez Hernán	Adquisiciones, DLOO	Planta
07817617-2	Cazenave González Luisa	Adquisiciones	-
07159035-6	Diaz Contreras Carlos	Contabilidad, Presupuesto	Planta
12832652-9	Muñoz Pasten Pamela	Adquisiciones	-

Fuente: Elaboración propia en base a la información proporcionada por la UTA.

Lo descrito no se aviene con lo establecido en 11.2 de la norma técnica NCh ISO 27.002, de 2009, relativo a la gestión del acceso de usuarios, el que dispone que deberían existir procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información y a los servicios, los cuales deberían cubrir todas las etapas de su ciclo de vida, es decir, desde su registro inicial hasta su cancelación.

A mayor abundamiento, es dable indicar que el numeral 11.2.1, que en su letra h), señala que tal procedimiento debería incluir el borrar o bloquear inmediatamente los derechos de acceso de los usuarios que hayan cambiado roles o tareas o dejado la organización.

En su respuesta, la Universidad indica que se procederá a implementar un procedimiento que permita, a la Dirección de Gestión Digital y Transparencia, contar con la información regular y periódica de la Dirección de Gestión de Personas y Bienestar de la Universidad, de forma tal, que se realice el control de la asignación de derechos de acceso a los sistemas de información y a los servicios.

A lo anterior, añade que adjunta el respaldo que da cuenta que los aludidos exfuncionarios ya no se encuentran activos en el aludido sistema.

Al respecto, atendido que la medida informada se materializará en el futuro y que no acredita que los exfuncionarios no se encuentran activos en la plataforma, se mantiene la observación.

Por lo anterior, la Universidad deberá remitir el respaldo fotográfico y documental, que acredite que las personas individualizadas en la tabla N° 6, no aparecen en los sistemas de dicha casa de estudios, además del procedimiento indicado en su respuesta, debidamente sancionado por la autoridad, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

18. Control de Acceso Remoto

La Universidad de Tarapacá no posee normas documentadas para el uso de acceso remoto, la que debe estar definida tanto

para usuarios y administradores, y debe contener una definición de las formas de acceder, servicios oficiales disponibles.

A mayor abundamiento, revisada la política de seguridad, se advierte que este tema no es abordado, ni mencionado en las secciones de control de acceso.

Lo indicado precedentemente, vulnera lo establecido la letra g) del artículo 37 del referido decreto N° 83, de 2004, que dispone, en síntesis, que se deberán realizar las estipulaciones de la sección 11.4 de la norma chilena de seguridad, donde deberán formalizarse en una política de uso correspondiente, de acuerdo con lo expresado en la sección "Política de Seguridad''.

Al respecto, dicho apartado dispone que el objetivo es prevenir el acceso no autorizado a los servicios en red, y que se debería controlar el acceso a los servicios en red, tanto internos como externos.

En este contexto, es dable manifestar que el numeral 11.4.2 establece que se deberían emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.

En su respuesta, la Universidad señala que procederá a formalizar e incorporar el procedimiento que acompaña, para poder solicitar control de acceso remoto en el proceso de actualización y complementación de la política de seguridad.

Sobre la materia, considerando que la acción comprometida se materializará en el futuro, se mantiene el alcance formulado.

En virtud de lo expuesto, la universidad deberá remitir el acto administrativo que apruebe el procedimiento que adjunta en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

19. Control de Acceso lógico para VPN

Si bien la Universidad de Tarapacá usa un software VPN para sus conexiones por la Red Privada Virtual y este posee medios criptográficos que protegen la confidencialidad e integridad de la información, los accesos por VPN deben cumplir con los requisitos formales de control de acceso lógico el cual no existe, vulnerando así lo establecido en la letra g) del artículo 37 del referido decreto N° 83, de 2004, que dispone, en síntesis, que se deberán realizar las estipulaciones de la sección 11.4 sobre control de acceso a la red y según lo dispuesto en el capítulo 11.1.1 política de control de acceso, de la norma NCh-ISO 27.002.

En sus descargos, la Universidad manifiesta que actualmente existe un software VPN (FortiNet) que permite acceder desde el exterior a la red de la institución, sin embargo, este no cuenta con un acceso lógico.

Añade, que la solicitud de acceso vía VPN se hace mediante correo electrónico y se registra en un formulario, lo cual respalda con a través de imágenes en su respuesta.

Finalmente, expone que procederá a formalizar un protocolo de control de acceso lógico por VPN considere lo dispuesto en la normativa individualizada precedentemente.

En virtud de lo expuesto, atendido que la universidad confirma el alcance formulado, y que la medida informada se materializará en el futuro, este se mantiene.

Por lo anterior, la Universidad deberá remitir el aludido protocolo, debidamente sancionado por la autoridad, en un plazo de 60 días hábiles contados desde la recepción del presente informe, por medio del Sistema de Seguimiento y Apoyo CGR.

20. Sobre los Softwares instalados

Respecto al inventario de equipos computacionales, entregado por la universidad de Tarapacá y la muestra analizada de 89 equipos, de los cuales se analizaron solo 73, debido a que el resto correspondiente a 16 equipos no se encontraron en la ubicación registrada, ni en sus cercanías, se verificó lo siguiente:

20.a Programa Winrar

Se encontraron 5 equipo con el software WinRAR instalado, los cuales se exponen a continuación.

Tabla N° 7: Equipos con Winrar instalado.

Código Bien	N° Serie	Tipo
53071118-1	5CD026MTKM	Notebook
53071164-1	5CG1140JLW	Notebook
53071253-1	MP27GX19	Notebook
53071228-3	5CD145BZ44	Notebook
53015945-25	67V8SZ2	Desktop

Fuente: Elaboración propia en base a las validaciones efectuadas en terreno.

Sobre la materia, cabe hacer presente que el programa Winrar versión de prueba, debe adquirirse o desinstalarse después de 40 días de uso al finalizar su periodo de evaluación o de prueba.

20.b Programas sin activar

Se encontraron 2 equipos con Microsoft office Profesional 2013, asociado al N° de inventario 53016016-1, y otro con Microsoft Visio 2016, inventario Nº 53071228-3, con la licencia sin activar.

20.c Programa sin Licencia

Se advirtió la existencia del equipo computacional con numero de inventario 53071228-3 con el programa PhantomPDF, el cual se encuentra expirado.

Las situaciones indicadas precedentemente vulneran lo establecido en la letra b) del artículo 22 del párrafo 7 del mencionado decreto N° 83, de 2004, que señala que, en todos los organismos sujetos a esa norma, deberán explicitarse y difundirse, entre otros, los antecedentes e información sobre gestión de las operaciones y las comunicaciones y las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado.

A mayor abundamiento, es del caso señalar que los artículos 19 y 20 de la ley N° 17.336, sobre Propiedad intelectual, disponen que nadie podrá utilizar públicamente una obra del dominio privado sin haber obtenido la autorización expresa del titular del derecho de autor, y que la infracción de lo dispuesto hará incurrir al o los responsables en las sanciones civiles y penales correspondientes.

En este contexto, cabe precisar la letra a), del artículo 79 de la referida ley N° 17.336, señala que, comete falta o delito contra la propiedad intelectual quién, sin estar expresamente facultado para ello, utilice obras de dominio ajeno protegidas por esta ley, inéditas o publicadas, en cualquiera de las formas o por cualquiera de los medios establecidos en el artículo 18 de esa misma normativa.

En cuanto a lo señalado en el numeral 20.a, la universidad señala que la unidad de soporte no instala el software Winrar en lo equipos, que en su lugar se usa el programa 7Zip, y que el Director de Servicios y Logística certificó la desinstalación del citado software.

A lo anterior, añade que procederá a implementar una directriz que asegure la gestión adecuada de software de prueba y su regularización antes del vencimiento del período de evaluación.

Al respecto, atendiendo que la Universidad no acompaña el respaldo que acredite la desinstalación del aludido programa y que la medida informada se materializará en el futuro, se mantiene la observación.

Luego, en cuanto al numeral 20.b, la Universidad manifiesta que se activaron las licencias de Microsoft Office Profesional 2013 y Microsoft Visio 2016, en los equipos correspondientes, según da cuenta el certificado emitido por el Director de la aludida dirección.

Sobre la materia, si bien la Universidad adjunta el mencionado certificado, el cual señala que se activó la licencia del equipo individualizado con el código de inventario N° 53016016-1, no es posible subsanar el alcance formulado, debido a que este documento no acredita la activación del

software, y porque señala que el otro bien no pudo ser verificado ya que presentaba una falla.

En virtud de lo expuesto, se mantiene la observación.

Por otra parte, en cuanto al numeral 20.c, la casa de estudios indica que se acompaña certificación del Director de Servicios y Logística, acreditando la desinstalación del programa PhantomPDF del equipo o la adquisición de la licencia correspondiente, y que se establecerá una política para monitorear y gestionar las licencias de software de forma continua.

En relación con lo anterior, el certificado al que hace referencia la Universidad en su respuesta, consigna que el equipo con código de inventario N° 53071228-3, presentó una falla, por lo que no pudo ser verificado, y no lo señalado en el párrafo precedente.

En atención a lo señalado, considerando que la Universidad no acredita la desinstalación del mencionado programa, y que la medida informada se materializará en el futuro, se mantiene la observación.

En relación con lo expuesto precedentemente, la casa de estudios deberá remitir los respaldos fotográficos que den cuenta de la desinstalación de los programas indicados en los numerales 20.a y 20.c, y de la activación de las licencias establecidas en el numeral 20.b, así como también, la política para monitorear y gestionar las licencias de forma continua, debidamente sancionada, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

21. Creación del Plan de Contingencia

Si bien la Universidad de Tarapacá cuenta con un plan de contingencia, documentado y formalizado, de acuerdo con el decreto exento Nº 267, de 30 de abril de 2020, no se advierte que su elaboración se haya ajustado al referido decreto Nº 83, de 2004.

Al respecto, el artículo 35 de ese texto normativo, dispone que el encargado de seguridad, que no se encuentra designado en la Universidad de Tarapacá, deberá formular un plan de contingencia para asegurar la continuidad de operaciones críticas para la institución.

Como recomendación, para llevar a cabo un plan de contingencia se debe formar un equipo de trabajo (como el comité de seguridad de la información) el cual debe incluir al encargado de seguridad, realizándose en primera instancia el “análisis de riesgo”, luego planificación de riesgos, impactos, probabilidades de que ocurra, posibles escenarios, y el “Desarrollo del plan”.

En su respuesta, la Universidad informa que, con ocasión de la formalización de la designación del Encargado de Seguridad, y

como parte de la mejora continua de la institución y del proceso de transformación digital, se procederá a actualizar el comité de seguridad, se realizará el análisis de riesgo, identificación de impactos, determinación de posibles escenarios y desarrollo de un plan de ejecución actualizado.

En virtud de lo expuesto, dado que las acciones informadas se materializarán en el futuro, y que el plan de contingencias fue elaborado sin ajustarse a la normativa individualizada precedentemente, se mantiene la observación.

Por lo anterior, la casa de estudios deberá remitir el plan de contingencia actualizado, debidamente formalizado, en un en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

22. Control de Valores

De la revisión efectuada a los módulos en los sistemas, se advirtieron deficiencias en algunos campos de los formularios, con respecto al largo de los textos con rango mayor a 256 caracteres, como por ejemplo el nombre y la dirección, lo que provocó falla en el ingreso de información dejando el navegador en estado de espera, vulnerando lo dispuesto en la letra f) del artículo 37, del decreto Nº 83, de 2004, referente a la gestión de las operaciones y comunicaciones y de acuerdo con lo dispuesto en la norma NCh-ISO 27.002, numeral 10.7.3 relativo al manejo de la información, el cual consigna en su letra d), que se debe asegurar que los datos de entrada estén completos, que el procesamiento se completa adecuadamente y que se valide su salida.

En su respuesta, la Universidad señala que, luego de la visita de la auditoría, se revisaron los sistemas y se aplicaron las observaciones identificadas en ese entonces, por lo que, actualmente no existen campos de formularios con largo mayor a 256 caracteres.

Añade, que, como parte de la mejora continua de la institución y el proceso de transformación digital, se realizó un catastro de todos los formularios de los sistemas de información, que contengan campos de formularios con extensión superior a 256 caracteres, subsanándose así la observación.

Al respecto, si bien se acogen los argumentos esgrimidos por la Universidad, esta no acompaña antecedentes que acrediten que el largo de los campos de los formularios no supera los 256 caracteres.

En virtud de lo expuesto, la casa de estudios deberá remitir el respaldo que acredite que los campos no exceden la anotada extensión o en caso contrario, que en estos no se genera error al ingresar texto, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

CONCLUSIONES

Atendidas las consideraciones expuestas durante el desarrollo del presente trabajo y el inicio de acciones, la Universidad de Tarapacá, ha aportado antecedentes que han podido salvar solo parte de las observaciones planteadas en el preinforme de auditoría N° 68, de 2023, de esta Entidad Fiscalizadora.

En efecto, las observaciones señaladas en el capítulo II, Examen de la Materia Auditada, numerales 2, referida a la inexistencia de un Encargado de seguridad; 5, sobre el comité de seguridad; 7, sobre activos sin registro de custodio; 8.a, literales i), ii), iii), iv), v) y vi), referidos a la seguridad física de la plataforma; 8.b, sobre los aires acondicionados de la sala de servidores; 8.c, literal i, relacionada con los cables de suministro de energía; y 8.d, sobre compra y mantención de arquitectura tecnológica, se dan por subsanadas, considerando las explicaciones y antecedentes aportados por la casa de estudios superiores.

A su turno, para las observaciones que se mantienen, la Universidad deberá adoptar las medidas pertinentes con el objeto de dar estricto cumplimiento a las normas legales y reglamentarias que la rigen, entre las cuales se estima necesario considerar, a lo menos, las siguientes:

1. En lo que atañe a lo señalado en el numeral 1 del Capítulo I, Aspectos de Control Interno, referido al sistema de proyectos sin actualizar (MC), la Universidad deberá remitir el respaldo que dé cuenta del cumplimiento de los hitos dispuestos en su carta Gantt, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

2. En relación a lo establecido en los numerales 3, y 4, relacionados con la gestión de riesgos (MC) y la Política de Seguridad (MC), respectivamente, ambas del Acápite II, Examen de la Materia Auditada, la Universidad deberá remitir la Política de Seguridad actualizada, debidamente sancionada por medio de acto administrativo, la que deberá consignar la periodicidad anual del desarrollo y revisión de la matriz de riesgo, y el cumplimiento del numeral 5.1.1 de la Norma Técnica NCh-ISO N° 27.002, de 2022, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

3. Respecto de lo indicado en el numeral 6.a del Acápite II, Examen de la Materia Auditada, sobre los equipos no informados (MC), la Universidad deberá remitir el acto administrativo que aprueba el instructivo emitido por la Dirección de Infraestructura y Equipamiento, y el respaldo que dé cuenta de la comunicación realizada a las unidades para el cumplimiento del Reglamento del Registro y Control de Bienes Muebles, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

4. En cuanto a lo expuesto en el numeral 6.b, del Acápite II, Examen de la Materia Auditada, sobre el control de inventario (MC), la universidad deberá adoptar las medidas de supervisión y control, que sean

necesarias, con el objeto de que se dé cumplimiento a las acciones comprometidas en sus descargos y con ello, a las disposiciones contenidas en el reglamento respectivo, ajustándose a las definiciones establecidas en el artículo 5°, de la resolución exenta N° 1.962, de 2022, que Aprueba Normas sobre Control Interno de la CGR.

5. Sobre lo establecido en el numeral 6.c, del Acápite II, Examen de la materia auditada, relacionado con las hojas de vida (MC), la Universidad deberá remitir la documentación que da cuenta de la materialización de la medida indicada en su respuesta, referida a la mejora al sistema de gestión de las hojas de vida, de manera que las fichas reflejen los cambios de ubicación históricos junto con los cambios de custodios de cada bien, en un plazo de 60 días hábiles contados desde la recepción del presente informe, lo que debe ser acreditado en el Sistema de Seguimiento y Apoyo CGR.

6. En relación con el numeral 6.d, del Acápite II, Examen de la materia auditada, sobre los responsables y ubicación de equipos (MC), la UTA deberá remitir el inventario de equipos con el detalle de los responsables, ubicación y el funcionario que los utiliza, en un plazo de 60 días hábiles contados desde la recepción del presente informe, lo que debe ser acreditado en el Sistema de Seguimiento y Apoyo CGR.

Asimismo, deberá adoptar las medidas de supervisión y control, que sean necesarias, con el objeto de que se dé cumplimiento a las acciones comprometidas en sus descargos, ajustándose a las definiciones establecidas en el artículo 5°, de la resolución exenta N° 1.962, de 2022, que Aprueba Normas sobre Control Interno de la CGR.

7. En relación con lo indicado en el literal ii), del numeral 8.c, del Acápite II, Examen de la materia auditada, sobre la rotulación de los interruptores de energía (MC), la Universidad deberá remitir el respaldo fotográfico que respalde la rotulación indicada, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

8. En cuanto a lo señalado en el numeral 9 del Capítulo II, Examen de la Materia Auditada, referida a la inexistencia de un procedimiento de destrucción de información (MC), la Universidad deberá remitir la política de destrucción de información, debidamente sancionada por acto administrativo, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

9. Respecto de lo indicado en numeral 10 del Capítulo II, Examen de la Materia Auditada, sobre la sociabilización de la política (MC), la Universidad deberá remitir los antecedentes que acrediten la implementación de las medidas informadas en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

10. Sobre lo expuesto en el numeral 11, relacionada con las deficiencias detectadas en los equipos (MC); 15, letras a), b), c), d), h), i) y k), asociadas a vulneraciones de las cuentas de usuarios detectadas en terreno (MC), y 16, sobre la estructura de contraseñas (MC), todas del Acápite II, Examen de la Materia Auditada, la Universidad deberá remitir la documentación de respaldo que acredite la implementación de las medidas informadas en su respuesta, esto es, de la revisión y ajustes de los permisos de las cuentas locales, la implementación de disposiciones que: prohíban permisos administrativos en cuentas no autorizadas; requieran contraseñas robustas para todas las cuentas, que incluyan longitud mínima y combinación de caracteres especiales, números y letras; sobre su cambio en forma periódica; sobre la nomenclatura estandarizada para todas las cuentas de usuario que facilite la identificación y control de acceso; de la configuración del sistema que obligue a la creación de contraseñas al configurar nuevas cuentas; de la creación de cuentas específicas para tareas administrativas y de la eliminación de aquellas genéricas; de acceso especiales para terceros, del establecimiento de controles críticos para la instalación de software; de una solución de gestión de aplicaciones que controlen y supervisen la instalación de software; y del marco integral de controles internos de TI, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR

11. En lo referido a los numerales 12, sobre el control de acceso a los equipos (MC), y 14, sobre la política de control de acceso (MC), ambas del Acápite II, Examen de la Materia Auditada, la casa de estudios deberá remitir la política de control de acceso a la información actualizada, y debidamente sancionada por acto administrativo, en los términos indicados en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

12. Según lo descrito en el numeral 13 del Acápite II, Examen de la Materia Auditada, sobre la integridad de los respaldos (MC), la Universidad remitir el procedimiento de respaldo de información que señala en su respuesta, debidamente sancionado por la autoridad, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

13. Respecto de lo indicado en el numeral 15, letras e) y f), del Acápite II, Examen de la Materia Auditada, sobre la inexistencia de controles por parte de la UDT (MC), la Universidad deberá remitir el detalle de los mecanismos de control implementados, junto con los antecedentes que lo acrediten, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

14. En cuanto a lo consignado en el numeral 15, letra g), del Acápite II, Examen de la Materia Auditada, sobre la inexistencia de administración de perfiles de usuario y de un administrador de sistema (MC), la Universidad deberá remitir la política de control de acceso de la información, que abarque la materia de la presente observación, y el acto administrativo que designe al “administrador de dominio, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

15. En relación con lo establecido en el numeral 15, letra j), del Acápite II, Examen de la Materia Auditada, sobre la implementación de reglas de control de acceso (MC), la universidad deberá remitir el detalle de los controles respectivos, junto con su documentación de respaldo, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

16. En lo que concierne al numeral 15, letras m) y n), del Acápite II, Examen de la materia auditada, sobre la inexistencia de un control de acceso lógico (MC) y la falta de un administrador de cuentas de usuario (MC), respectivamente, la universidad deberá remitir la política debidamente sancionada por la autoridad, y la documentación que acredite la implementación del control de acceso lógico ante cambio de funciones, destitución u otra variación que pueda experimentar la relación de un funcionario en la institución, y de la actualización del administrador de cuentas para usuario, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

17. En cuanto a lo indicado en el numeral 17 del Acápite II, Examen de la Materia Auditada, sobre usuarios desvinculados activos en sistemas (MC), la UTA deberá remitir el respaldo fotográfico y documental, que acredita que las personas individualizadas en la tabla N° 6, no aparecen en los sistemas de dicha casa de estudios, además del procedimiento indicado en su respuesta, debidamente sancionado por la autoridad, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

18. De acuerdo con lo señalado en el numeral 18 del Acápite II, Examen de la materia auditada, relacionado con el control de acceso remoto (MC), la universidad deberá remitir el acto administrativo que apruebe el procedimiento que adjunta en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

19. En cuanto al numeral 19 del Acápite II, Examen de la Materia Auditada, referido al control de acceso lógico para VPN (MC), la universidad deberá remitir el protocolo indicado en su respuesta, debidamente sancionado por la autoridad, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

20. Sobre lo expuesto en los numerales 20.a, 20.b y 20.c, del Acápite II, Examen de la Materia Auditada, sobre los programas instalados (C), la universidad deberá remitir los respaldos fotográficos que den cuenta de la desinstalación del programa Winrar de los equipos indicados en la tabla N° 7, y del software PhantomPDF, del bien individualizado con el código de inventario N° 53071228-3, y de la activación de las licencias de Microsoft office Profesional 2013 y Microsoft Visio 2016, de los computadores asociados al N° de inventario 53016016-1, y Nº 53071228-3, respectivamente, así como también, la política para monitorear y gestionar las licencias de forma continua, debidamente sancionada, en un plazo de

60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

21. Sobre lo expuesto en el numeral 21, sobre la creación del Plan de Contingencia (MC), la Universidad deberá remitir el plan de contingencia actualizado, debidamente formalizado, en un en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

22. En relación con el numeral 22, del Acápite II, Examen de la Materia Auditada, referido al control de valores (MC), la casa de estudios deberá remitir el respaldo que dé cuenta que los campos no exceden la anotada extensión o en caso contrario, que en estos no se genera error al ingresar texto, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

Respecto de aquellas observaciones que se mantienen y que fueron categorizadas como MC y/o LC en el citado “Informe de Estado de Observaciones”, el cumplimiento de las acciones correctivas requeridas deberá ser informado por las unidades responsables al Encargado de Control/Auditor Interno, a través del Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, quien a su vez deberá acreditar y validar en los siguientes 30 días hábiles la información cargada en la ya mencionada plataforma, de conformidad a lo establecido en el aludido oficio N° 14.100, de 2018.

Remítase al Rector y a la Contralora (s), ambos de la Universidad de Tarapacá.

Saluda atentamente a Ud.,

Firmado electrónicamente por:	
Nombre:	VICTOR ESTEBAN TORRES TORRES
Cargo:	Jefe de Unidad de Control Externo
Fecha:	29/04/2025

Anexo N° 1: Equipos no encontrados

Código	Ubicación	Serie	Tipo
53015969-3	Bodega central FACSAL	8CG0253PYT	Desktop
53071215-2	Dosimetría (of. Académico Carlos Úbeda)	5CG147DSCO	Notebook
53015959-1	Lab. De modelamiento matemático, nanociencia y física	DC2019072500485	Desktop
53071274-4	Modulo N.º 16 - académico	5CD202BXV1	Notebook
53009771-1	Of. Investigador 1 Depto. Jv Lastarria	BDZZMV2	Notebook
53016046-10	Of. N.º 2 profesores hora - acad. Liliana Cañipa trigo	8CC15170DZ	Desktop
53071215-3	Of. N.º 2 profesores hora - acad. Maura Auad Brito	5CG147DSBG	Notebook
53015966-2	Of. Profesionales. Secretaria de la universidad	GX2YH03	Desktop
53071152-2	Oficina - Misael Camus	LR0E7P7Y	Notebook
53015945-24	Oficina del director	6756SZ2	Desktop
53071207-1	Oficina N.º 16 académico - Cesar Cisneros	PF30HQE4	Notebook
53071159-1	Oficina Nº 9 académica - Mariana Leon	SCD11722LF	Notebook
53015951-1	Oficina secretaria dirección depto. Jv Lastarria	HCLT7X2	Desktop
53071252-4	Pasillo interior	PF2SAHTR	Notebook
53071156-1	Sala de reuniones doctorado (anexo biblioteca)	M3N0CX05D80410F	Notebook
53071156-3	Sala de reuniones doctorado (anexo biblioteca)	M3N0CX05D82310E	Notebook

Fuente: Elaboración propia en base a las validaciones efectuadas en terreno y a ubicación de los equipos entregados en el inventario de la Universidad de Tarapacá.

Anexo Nº 2: Equipos sin custodio

Código	Tipo	Ubicación	Serie
53016041-1	Desktop	Oficina N° 10 Academica - Liliana Pedraja	CO2FTO2LQ6W2
53016044-1	Desktop	Oficina Decano	8CG9502F4Y
53016044-2	Desktop	Oficina secretaria	8CG9502F43
53016044-3	Desktop	Oficina Encargada Administrativa	8CG9502F4S
53016044-4	Desktop	Oficina académico - Nelson Lara	8CG9502F5Q
53016044-5	Desktop	Oficina académico - Nelson Lara	8CG9502F3Q
53016044-6	Desktop	Sala De Clases N° 202	8CG9502F57
53016044-7	Desktop	Oficina Académica - Delia Laime	8CG9502F68
53016044-8	Desktop	Oficina secretaria Jefatura Carrera	8CG9502F4J
53016044-9	Desktop	Of. 8 - Maria Ester Onell	8CG9502F5V
53016045-1	Desktop	Oficina Académica - Juana Mamani	8CG9502F5G
53016046-1	Desktop	Oficina secretaria	8CC1517089
53016046-2	Desktop	Oficina secretaria	8CC15170B1
53016046-3	Desktop	Oficina secretaria	8CC15170GJ
53016046-4	Desktop	Laboratorio Banco De Sangre	8CC151700K
53016046-5	Desktop	Oficina Nº 9 Academica - Mariana Leon	8CC151709X
53016046-6	Desktop	Oficina N.º 8 Académica - Natalia Herrera Medina	8CC15170B3
53016046-7	Desktop	Oficina N.º 10 académica - Andrea Inchausti Daza	8CC151701Z
53016046-8	Desktop	Oficina N.º 1 académica - Teresa Reyes Rubilar	8CC15170CQ
53016046-9	Desktop	Oficina Nº 11 Academica - Ana Maria Naranjo Garate	8CC15170GG
53016046-10	Desktop	Of. N.º 2 Profesores Hora - Acad. Liliana Cañipa Trigo	8CC15170DZ
53016046-11	Desktop	Oficina N.º 7 Academica - Katina Latorre Progulakis	8CC151709N
53016046-12	Desktop	Oficina Nº 8 Academica - Ximena Figueroa Jimenez	8CC15170CF
53016046-13	Desktop	Oficina N.º 11 académico - Juan Ventura Ventura	8CC15170F0
53016047-1	Desktop	Pasillo Interior	20WW1BRT60
53016052-1	Desktop	Of. Secretaria	8CC1521V8J
53016052-2	Desktop	Of. Secretaria De Carrera	8CC1521V8D
53016052-3	Desktop	Of. Secretaria	8CC151704Y
53016052-4	Desktop	Of. Secretaria	8CC1521V56
53016052-5	Desktop	Of. Secretaria	8CC1521V5G
53016052-6	Desktop	Of. Secretaria	8CC1521V5S
53016052-7	Desktop	Of. Secretaria	8CC1521V89
53016052-8	Desktop	Of. Secretaria	8CC151706C
53016052-9	Desktop	Of. Secretaria	8CC1521V5H
53016052-10	Desktop	Of. Secretaria	8CC151704J
53016054-1	Desktop	Oficina académica - Monica Navarrete	YJ01C0WP
53016055-1	Desktop	Modulo Nº 2 - Dr. Pedro Hecht	4CE116XRZ5
53016056-1	Desktop	Oficina académico - Carlos Ruiz	MP1ZE57L
53016057-1	Desktop	Oficina del director	4CE116XRQ8
53016058-1	Desktop	Oficina Director, Dirección General De Gabinete	MP1Z2SP8
53016059-1	Desktop	Oficina - Oliver Meseguer	C02G40RUPN5W

Código	Tipo	Ubicación	Serie
53016060-1	Desktop	Secretaria - Sala De Espera D.A.E.	8CN1380L0F
53016060-2	Desktop	Oficina Víctor Flores - Asistencia Social	8CN1380KHD
53016060-3	Desktop	Sala De Procedimientos Of. De Salud Estudiantil	8CN1380KGV
53016060-4	Desktop	Oficina Pamela Alday - Asistencia Social	8CN1380KZC
53016060-5	Desktop	Of. Priscilla Toro - Asistencia Social (Velásquez)	8CN1380KZ8
53016060-6	Desktop	Oficina Director D.A.E.	8CN1380L09
53016060-7	Desktop	Oficina Yasmin Araya - Asistencia Social	8CN1380KZG
53016060-8	Desktop	Oficina Cintia Vergara - Asistencia Social	8CN1380KZT
53016060-9	Desktop	Oficina Coordinadora De Salud Estudiantil	8CN1380KZM
53016060-10	Desktop	Oficina Secretaria - Asistencia Social	8CN1380KJD
53016060-11	Desktop	Of. Coordinadora Carla Correa - Asistencia Social	8CN1380KJT
53016061-1	Desktop	Oficina Secretaria Jefatura De Carrera	8CC204224D
53016061-2	Desktop	Oficina Secretaria Jefatura De Carrera	8CC2042248
53016061-3	Desktop	Oficina Secretaria Jefatura De Carrera	8CC1516ZX0
53016061-4	Desktop	Oficina Nº 3 Secretaria	8CC1516ZWJ
53016061-5	Desktop	Recepción	8CC1516ZVJ
53016061-6	Desktop	Recepción	8CC1516ZWG
53016061-7	Desktop	Oficina Nº 28 Secretaria Departamento De Kinesiología Y Nutrición	8CC1516ZKM
53016061-8	Desktop	Oficina Nº 3 Secretaria Jefatura De Carrera	8CC204224Y
53016061-9	Desktop	Oficina Nº 29 Director Departamento De Kinesiología Y Nutrición	8CC1516ZZ0
53016061-10	Desktop	Oficina Secretaria	8CC204220R
53016061-11	Desktop	Oficina Nº 4 Académica - Marisell Correa Butron	8CC1516ZZD
53016061-12	Desktop	Oficina Nº 15 - Secretaria	8CC1517029
53016061-13	Desktop	Oficina Nº 14 - Directora	8CC1516ZWT
53016061-14	Desktop	Oficina Nº 10 Académica - Andrea Inchausti Daza	8CC1516ZVC
53016061-15	Desktop	Oficina Nº 8 Secretaria Jefatura De Carrrera	8CC2042234
53016064-1	Desktop	Oficina - Alberto Diaz	MP1ZCV23
53016067-1	Desktop	Oficina De Publicaciones	MP211RAQ
53016068-1	Desktop	Oficina Nº 2 - Director	MP21K7SK
53016068-2	Desktop	Oficina Nº 2 - Director	MP21K40J
53016068-3	Desktop	Oficina Nº 2 - Director	MP21K40D
53016071-1	Desktop	Oficina Académico - Daniel Vera	8CC1500P6B
53016071-2	Desktop	Oficina Secretaria	8CC1500P22
53071188-1	Notebook	Oficina N° 12 - Octavio Vera	C02XTOTAJK77
53071231-1	Notebook	Laboratorio De Ecología Acuática N° 1	C02G92S7Q05F
53071232-1	Notebook	Lab. Biología Del Cáncer, Molecular E histopatología	PF2SD3SJ
53071241-1	Notebook	Oficina Vicerrector Académico	F3ZZYH3
53071241-2	Notebook	Oficina Vicerrector Académico	6JHYYH3
53071242-1	Notebook	Oficina Académica - Carmen Seguel	5CG1401K5T
53071244-1	Notebook	Oficina Decano	M9N0CX15K349372

Código	Tipo	Ubicación	Serie
53071245-1	Notebook	Oficina Decanatura	5CD1514WXX
53071245-2	Notebook	Oficina Encargado Administrativo	5CD146GPM4
53071246-1	Notebook	Oficina Académico - Pablo Valladares	K2109N0065878
53071247-1	Notebook	Oficina Académico - Arnaldo Ortega (Jefe De Carrera)	PF347S16
53071248-1	Notebook	Oficina N° 13 Académico - Juan Vega	PF31HL1F
53071249-1	Notebook	Oficina Director	PF2TKRD8
53071250-1	Notebook	Oficina N° 10 Académica - Liliana Pedraja	C02GV0Z0Q05H
53071252-1	Notebook	Pasillo Interior	PF2SAHSK
53071252-2	Notebook	Pasillo Interior	PF2SAHSG
53071252-3	Notebook	Pasillo Interior	PF2SAFKF
53071252-4	Notebook	Pasillo Interior	PF2SAHTR
53071253-1	Notebook	Of. Profesionales Otl	MP27GX19
53071254-1	Notebook	Oficina N° 10 - Académico Cristian Pinto	C02GXLVFQ05D
53071255-1	Notebook	Oficina Nº 2 - Director	5CD202BXSV
53071255-2	Notebook	Oficina Nº 12 - Juan Carlos Mamani	5CD202BXSS
53071255-3	Notebook	Oficina Nº 6 - Miria Luque	5CD202BXSO
53071255-4	Notebook	Pasillo Interior	5CD202BXSP
53071255-5	Notebook	Pasillo Interior	5CD202BXQZ
53071255-6	Notebook	Oficina Nº 22 - Vilma Arevalo Lancellotti	5CD202BXSJ
53071255-7	Notebook	Oficina Nº 22 - Vilma Arevalo Lancellotti	5CD202BXSN
53071255-8	Notebook	Oficina Secretaria	5CD202BXSG
53071255-9	Notebook	Oficina Encargado Administrativo	5CD202BXKQ
53071255-10	Notebook	Oficina Encargado Administrativo	5CD202BXRM
53071256-1	Notebook	Of. 11 - Ana Cabanas	FH7GQNH6T2
53071257-1	Notebook	Oficina Director David Laroze	C07GX1R7Q6NW
53071258-1	Notebook	Of. Profesionales, Dir. De Investigación, Postgrado Y Transferencia Tecnológica	MP22G08K
53071259-1	Notebook	Oficina N° 14 - Liliana Hernandez	K2109N0065916
53071260-1	Notebook	Laboratorio De Electronica	PF31DFRZ
53071262-1	Notebook	Oficina Nº 2 Académica - Jessica Moreno Garces	5CD202BXDK
53071262-2	Notebook	Oficina Nº 8 Académica - Maria Gonzalez Flores	5CD202BXMM
53071262-3	Notebook	Oficina Nº 3 Secretaria	5CD202BXH6
53071264-1	Notebook	Of. Doctorado En Educación (Anexo Biblioteca) 2do. Piso	PF2SAHSK
53071265-1	Notebook	Oficina N° 13 - Academico Alejandro Cuadra	8CG1458BGZ
53071269-1	Notebook	Oficina Nº 23 - Director	8KRT1J3
53071274-1	Notebook	Modulo Nº 21 - Dra. Daniela Jimenez	5CD202BZ11
53071274-2	Notebook	Modulo Nº 1 - Dr. Eduardo Parra	5CD202BZ1K
53071274-3	Notebook	Modulo Nº 7 - Dra. Adriana Sapiro	5CD202BXQ4
53071274-4	Notebook	Modulo Nº 16 - Académico	5CD202BXV1
53071274-5	Notebook	Modulo Nº 8 - Académico	5CD202BYZL
53071274-6	Notebook	Modulo Nº 8 - Académico	5CD202BYZ6
53071274-7	Notebook	Modulo Nº 18 - Académico	5CD202BYZZ
53071275-1	Notebook	Oficina Académico - Ernesto Ponce	5CD2103Y0P

Fuente: Elaboración propia en base a los antecedentes proporcionados por la Universidad de Tarapacá.

Anexo N° 3: Estado de Observaciones de Informe Final N° 68, de 2023

OBSERVACIONES QUE SERÁN VALIDADAS POR EL ENCARGADO DE CONTROL INTERNO DE LA ENTIDAD

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN
Capítulo I, Aspectos de Control Interno, numeral 1.	Sistema de gestión de proyectos sin actualizar	MC: Medianamente Compleja	La universidad deberá remitir el respaldo que de cuenta del cumplimiento de los hitos dispuestos en su carta Gantt, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 3.	En relación a la gestión de riesgos	MC: Medianamente Compleja	La universidad deberá remitir la Política de Seguridad actualizada, debidamente sancionada por medio de acto administrativo, la que deberá consignar la periodicidad anual del desarrollo y revisión de la matriz de riesgo, y el cumplimiento del numeral 5.1.1 de la Norma Técnica NCh-ISO N° 27.002, de 2022, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 4.	En cuanto a la política de seguridad	MC: Medianamente Compleja	
Capítulo II, Examen de la Materia Auditada, numeral 6.a	Sobre los equipos no informados	MC: Medianamente Compleja	La universidad deberá remitir el acto administrativo que aprueba el instructivo emitido por la Dirección de Infraestructura y Equipamiento, y el respaldo que de cuenta de la comunicación realizada a las unidades para el cumplimiento del Reglamento del Registro y Control de Bienes Muebles, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 6.c	En relación con las hojas de vida	MC: Medianamente Compleja	La universidad deberá remitir la documentación que da cuenta de la materialización de la medida indicada en su respuesta, referida a la mejora al sistema de gestión de las hojas de vida, de manera que las fichas reflejen los cambios de ubicación históricos junto con los cambios de custodios de cada bien, en un plazo de 60 días hábiles contados desde la recepción del presente informe, lo que debe ser acreditado en el Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 6.d	Sobre los responsables y ubicación de equipos	MC: Medianamente Compleja	La UTA deberá remitir el inventario de equipos con el detalle de los responsables, ubicación y el funcionario que los utiliza, en un plazo de 60 días hábiles contados desde la recepción del presente informe, lo que debe ser acreditado en el Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 8.c, literal ii)	Sobre la rotulación de los interruptores de energía	MC: Medianamente Compleja	La universidad deberá remitir el respaldo fotográfico que respalde la rotulación indicada, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN
Capítulo II, Examen de la Materia Auditada, numeral 9.	Respecto a la inexistencia de un procedimiento de destrucción de información.	MC: Medianamente Compleja	La universidad deberá remitir la política de destrucción de información, debidamente sancionada por acto administrativo, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 10.	Sobre la sociabilización de la política	MC: Medianamente Compleja	La universidad deberá remitir los antecedentes que acrediten la implementación de las medidas informadas en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 11.	Relacionada con las deficiencias detectadas en los equipos	MC: Medianamente Compleja	La universidad deberá remitir la documentación de respaldo que acredite la implementación de las medidas informadas en su respuesta, esto es, de la revisión y ajustes de los permisos de las cuentas locales, la implementación de disposiciones que: prohíban permisos administrativos en cuentas no autorizadas; requieran contraseñas robustas para todas las cuentas, que incluyan longitud mínima y combinación de caracteres especiales, números y letras; sobre su cambio en forma periódica; sobre la nomenclatura estandarizada para todas las cuentas de usuario que facilite la identificación y control de acceso; de la configuración del sistema que obligue a la creación de contraseñas al configurar nuevas cuentas; de la creación de cuentas específicas para tareas administrativas y de la eliminación de aquellas genéricas; de acceso especiales para terceros, del establecimiento de controles críticos para la instalación de software; de una solución de gestión de aplicaciones que controlen y supervisen la instalación de software; y del marco integral de controles internos de TI, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 15. letras a), b), c), d), h), i) y k)	Asociadas a vulneraciones de las cuentas de usuarios detectadas en terreno	MC: Medianamente Compleja	
Capítulo II, Examen de la Materia Auditada, numeral 16.	Sobre la estructura de las contraseñas	MC: Medianamente Compleja	
Capítulo II, Examen de la Materia Auditada, numeral 12.	Sobre al control de acceso a los equipos	MC: Medianamente Compleja	La UTA deberá remitir la política de control de acceso a la información actualizada, y debidamente sancionada por acto administrativo, en los términos indicados en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 14.	Sobre la política de control de acceso	MC: Medianamente Compleja	
Capítulo II, Examen de la Materia Auditada, numeral 13.	Sobre la integridad de los respaldos	MC: Medianamente Compleja	La universidad remitir el procedimiento de respaldo de información que señala en su respuesta, debidamente sancionado por la autoridad, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 15, letras e) y f)	Sobre la inexistencia de controles por parte de la UDT	MC: Medianamente Compleja	La Universidad deberá remitir el detalle de los mecanismos de control implementados, junto con los antecedentes que lo acrediten, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN
Capítulo II, Examen de la Materia Auditada, numeral 15, letra g)	Sobre la inexistencia de administración de perfiles de usuario y de un administrador de sistema	MC: Medianamente Compleja	La Universidad deberá remitir la política de control de acceso de la información, que abarque la materia de la presente observación, y el acto administrativo que designe al "administrador de dominio, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 15, letra j)	Sobre la implementación de reglas de control de acceso	MC: Medianamente Compleja	La universidad deberá remitir el detalle de los controles respectivos, junto con su documentación de respaldo, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 15, letra m)	Sobre la inexistencia de un control de acceso lógico	MC: Medianamente Compleja	La universidad deberá remitir la política debidamente sancionada por la autoridad, y la documentación que acredite la implementación del control de acceso lógico ante cambio de funciones, destitución u otra variación que pueda experimentar la relación de un funcionario en la institución, y de la actualización del administrador de cuentas para usuario, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 15, letra n)	En cuanto a la falta de un administrador de cuentas de usuario	MC: Medianamente Compleja	
Capítulo II, Examen de la Materia Auditada, numeral 17.	Sobre usuarios desvinculados activos en sistemas	MC: Medianamente Compleja	La UTA deberá remitir el respaldo fotográfico y documental, que acredita que las personas individualizadas en la tabla N° 6, no aparecen en los sistemas de dicha casa de estudios, además del procedimiento indicado en su respuesta, debidamente sancionado por la autoridad, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 18.	Relacionado con el control de acceso remoto	MC: Medianamente Compleja	La universidad deberá remitir el acto administrativo que apruebe el procedimiento que adjunta en su respuesta, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 19.	Referido al control de acceso lógico para VPN	MC: Medianamente Compleja	La universidad deberá remitir el protocolo indicado en su respuesta, debidamente sancionado por la autoridad, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numerales 20.b, 20.b y 20.c	Sobre los programas instalados	MC: Medianamente Compleja	La universidad deberá remitir los respaldos fotográficos que den cuenta de la desinstalación del programa Winrar de los equipos indicados en la tabla N° 7, y del software PhantomPDF, del bien individualizado con el código de inventario N° 53071228-3, y de la activación de las licencias de Microsoft office Profesional 2013 y Microsoft Visio 2016, de los computadores asociados al N° de

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN
			inventario 53016016-1, y Nº 53071228-3, respectivamente, así como también, la política para monitorear y gestionar las licencias de forma continua, debidamente sancionada, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 21.	Sobre la creación del Plan de Contingencia	MC: Medianamente Compleja	La UTA deberá remitir el plan de contingencia actualizado, debidamente formalizado, en un en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.
Capítulo II, Examen de la Materia Auditada, numeral 22	Referido al control de valores	MC: Medianamente Compleja	La UTA deberá remitir el respaldo que de cuenta que los campos no exceden la anotada extensión o en caso contrario, que en estos no se genera error al ingresar texto, en un plazo de 60 días hábiles contados desde la recepción del presente informe, a través del Sistema de Seguimiento y Apoyo CGR.

Fuente: Elaboración propia en base a la respuesta entregada por la Universidad de Tarapacá.