ANTECEDENTES GENERALES

Este procedimiento forma parte de las guías de acción definidas por la Contraloría para auditar los procesos de Administración y desarrollo de TIC en la Universidad de Valparaíso.

OBJETIVO

Administrar de manera estandarizada los objetivos de control de las Auditorías que se desarrollen sobre las Unidades de la Universidad que lleven a cabo procesos de Administración y Desarrollo de Tecnologías de Información.

ALCANCE

Este procedimiento permite auditar de manera cabal las actividades de DISICO, y de cualquier otra Unidad de la Universidad que tenga a su cargo la administración o desarrollo de tecnologías de información.

AUTORIDADES Y RESPONSABLES

El siguiente, constituye la definición de roles y responsabilidades asignadas a los agentes involucrados en la gestión de fraude, a nivel de las TI:

Contralor: Jefe Superior del organismo, responsable de planificar, organizar y dirigir el funcionamiento de la Contraloría Interna.
Jefe del Departamento de Control de la Gestión Institucional: Jefatura del Área de Control de Gestión Institucional de la Contraloría Interna, responsable de la planificación, administración y supervisión del trabajo del equipo de Auditores de la Universidad de Valparaíso.

Auditor Resguardo Patrimonial: Profesional de la Contraloría Interna, responsable de administrar y auditar los riesgos de Daño Patrimonial de la Institución.

Auditor Staff: Profesional de la Contraloría Interna asignado para la ejecución del trabajo en terreno y emisión de informes.

Comisión de Administración de Riesgos: Es el encargado de aprobar los planes de acción propuestos para mitigar los hallazgos de la Contraloría General de la República.

Auditor de TI: Profesional de la Contraloría responsable de administrar y auditar los riesgos de TI de la Institución.

COPIA CONTROLADA

CONDICIONES GENERALES

1. El programa de inspecciones de las TIC se basa en los objetivos de control definidos por COBIT (Control Objetives for Information and related technologies), que define una base de referencia conceptual, reconocida a nivel de la Industria como marco de trabajo para las Auditorías de Tecnologías de Información.

2. El Auditor TI desarrolla de manera anual el Programa de Auditoría TI, consistente en una Carta Gantt destinada a definir las actividades de Auditoría que se ejecutarán en el ámbito de las TI en las Unidades seleccionadas de la Universidad. Este procedimiento sirve como referencia para la ejecución de las Auditorías definidas en el dicho Programa.

3. La Contraloría General de la República realiza Auditorías de manera no programada. Estas son realizadas sin la participación de la Contraloría Interna.

4. Los informes de la Contraloría General incluyen las observaciones del informe anterior que no hayan sido solucionadas, observando los avances que se hayan realizado al respecto. Por este motivo, no se hace necesario revisar informes anteriores para revisar los temas pendientes de resolver observados por la Contraloría.

5. La Contraloría General de la República analiza el cumplimiento de la reglamentación vigente en relación a los temas de TI. En particular el decreto 83 de 2004, establece los requisitos que deben cumplir las Instituciones Estatales en relación a las TICs. Desde este punto de vista la Auditoría busca principalmente encontrar irregularidades a nivel de forma.

6. La Contraloría General audita los procesos centrales de la Universidad, por lo cual la Contraloría Interna podrá auditar de manera selectiva, los hallazgos detectados a nivel de las Facultades.

7. La Contraloría Interna no tiene como objetivo Auditar el cumplimiento de los tópicos analizados por la Contraloría General de la República, como tampoco evaluar el grado de pertinencia o completitud de sus análisis.

8. Las Auditorías Externas son contratadas por parte de las Autoridades Administrativas de la Universidad, con el fin de analizar el nivel de cumplimiento de los procesos de la Universidad con las buenas prácticas de la Industria y con evaluar el grado de cumplimiento existente con sus propias políticas y procedimientos.

9. Los informes de las Empresas Externas incluyen las observaciones del informe anterior que no hayan sido solucionadas, indicando los avances que se hayan realizado al respecto. Por este motivo, no se hace necesario revisar informes anteriores para revisar los temas pendientes de resolver observados por la Empresa Externa.

V°B° CONTRALOR

10. La Empresa Externa audita principalmente los procesos centrales de la Universidad, por lo cual la Contraloría Interna podrá auditar de manera selectiva, los hallazgos detectados a nivel de las Facultades.

11. Los riesgos potenciales de fraude a nivel de las TI pueden ser de diferente naturaleza:

    a. Riesgos asociados a la pérdida de recursos patrimoniales por uso malicioso de las TI.

    b. Riesgos asociados a debilidades en las políticas y procedimientos de TI.

    c. Riesgos asociados a una operación defectuosa de los sistemas, por falta de rigurosidad de los procesos de certificación.

    d. Riesgos de seguridad asociados a conexiones indebidas a través de la redes de la Universidad.

    e. Riesgos asociados a la administración deficiente de los recursos TI por parte de las Unidades de la Universidad.

12. Para el desarrollo de los análisis técnicos asociados a los riesgos, así como la identificación de potenciales nuevos riesgos, el Auditor hará uso de tecnologías de información provistas para tal efecto:

    a. Herramientas de Auditoría Asistida por Computador, como apoyo a los procesos de muestreo, generación de datos de pruebas y detección automática de fraudes, identificación de patrones de comportamiento de fraude.

    b. Acceso a los sistemas de la Universidad a través de bases espejo de los sistemas productivos.

    c. Acceso a los componentes fuentes de las aplicaciones, asociados a los sistemas productivos o asociados a respaldos de versiones anteriores.

    d. Acceso a las bitácoras de los sistemas computacionales y a la configuración de los sistemas de administración computacionales.

13. La Auditoría de procesos de la Contraloría es responsable por administrar la Matriz de Riesgo Operativa de la Universidad.

COPIA CONTROLADA

V°B° CONTRALOR

EQUIPOS, HERRAMIENTAS Y MATERIALES

1. La contraloría Interna cuenta con un sistema, llamado PAWS, utilizado para registrar y monitorear las matrices de riesgo de la Universidad.

2. Para el desarrollo de los análisis técnicos, así como la identificación de potenciales nuevos riesgos, el Auditor hará uso de tecnologías de información provistas para tal efecto:

    a. Herramientas de Auditoría Asistida por Computador, como apoyo a los procesos de muestreo, generación de datos de pruebas y detección automática de fraudes, identificación de patrones de comportamiento de fraude.

    b. Acceso a los sistemas de la Universidad a través de bases espejo de los sistemas productivos.

    c. Acceso a los componentes fuentes de las aplicaciones, asociados a los sistemas productivos o asociados a respaldos de versiones anteriores.

    d. Acceso a las bitácoras de los sistemas computacionales y a la configuración de los sistemas de administración computacionales.

3. La contraloría cuenta con acceso a todos los sistemas y a las bases de datos de la Universidad.

4. La contraloría cuenta con el software ACL, que permite a los auditores ejecutar pruebas de auditoría y obtener muestras de manera automatizada, debiendo para esto cargar los datos desde los sistemas fuente de la Universidad en el equipo del Auditor TI.

COPIA CONTROLADA

V°B° CONTRALOR

DESCRIPCIÓN DEL PROCEDIMIENTO (Narrativa)

Ejecución del Programa de Inspección de las TIC

ACTIVIDAD 1:

ETAPA DE PLANIFICACIÓN: De acuerdo al Manual de Auditoría, se define la planificación de la Auditoría completando el Formulario N°1 "Planificación de Auditoría".

En esta etapa se definen:

- Objetivo General y específicos de la Auditoría.
- Alcance de la auditoría, (período y universo muestral a auditar).
- Equipo de Auditores
- Tiempo definido para la auditoría
- Pruebas de auditoría a aplicar
- Antecedentes a solicitar

ACTIVIDAD 2:

ETAPA DE EJECUCIÓN DE LA AUDITORIA:

1. El profesional asignado a la ejecución de la Auditoría, realiza las reuniones con las personas asignadas. Realizando las indagaciones indicadas en la planilla "Programa de Auditorias TI", y documentando en la misma planilla los resultados de sus actividades.

2. El auditor asignado, debe realizar un relevamiento sobre el área auditada, con el objetivo de identificar:

   a. Sistemas informáticos utilizados por el área auditada: se deben identificar tanto los sistemas administrados por DISICO como aquellos que sean administrados por personal interno al área auditada.

   b. Bases de datos utilizadas: se deben identificar las fuentes utilizadas de información, tanto a nivel interno como externo al área auditada como de la Universidad.

   c. Personal y responsabilidades sobre las TIC: se identifican en esta etapa los funcionarios y funciones relacionadas con el desarrollo y administración de las TIC al interior del área auditada.

COPIA CONTROLADA

V°B° CONTRALOR

d. Proyectos y recursos asignados del área auditada, destinados al desarrollo de TIC.

3. En relación a los sistemas existentes, se realizan los siguientes análisis:

   a. Existencia de otros sistemas en la Universidad que cumplen con la funcionalidad que el sistema contempla.

   b. De acuerdo al nivel de relevancia del sistema para la Unidad auditada, determinar y evaluar el nivel de continuidad operacional existente (existencia de respaldos y planes de contingencia).

   c. Analizar si la participación de DISICO en el desarrollo y administración del sistema.

4. En relación a las bases de datos existentes, se debe analizar:

   a. Nivel de Consistencia de las bases de datos existentes con las bases de datos corporativas.

   b. Niveles de seguridad y acceso de acuerdo a los requerimientos de la Unidad.

   c. Controles asociados a cambios sobre las bases de datos.

5. En relación al personal y responsabilidades en el ámbito de las TIC, se debe analizar:

   a. Personal que realice funciones de administración y desarrollo de las TIC fuera del ámbito de dependencia de DISICO.

   b. Nivel de capacitación del personal que realice funciones de administración y desarrollo de las TIC.

6. En relación a los proyectos y recursos destinados a las TIC, se debe analizar:

   a. Nivel de cumplimiento del presupuesto definido para Ingresos y Gastos en el ámbito de las TIC.

   b. Correspondencia, en términos cuantitativos y cualitativos, entre los recursos ejecutados y comprometidos y los productos y servicios adquiridos por la Unidad auditada.

COPIA CONTROLADA

V°B° CONTRALOR

ACTIVIDAD 3:

ETAPA DE ELABORACIÓN DEL PREINFORME E INFORME FINAL:

1. Auditor TI prepara pre-Informe de Inspección de las TIC. La estructura del Informe se ajustará a lo establecido en el Manual de Auditoría.
2. Se someterá el Pre-Informe a Revisión de Jefatura del Departamento de Control de la Gestión Institucional.
3. Auditor TI incorpora las correcciones, cambios y/o mejoras propuestos por la Jefatura y emite el Informe final de auditoría.
4. El Jefe del Departamento de Control de la Gestión Institucional aprueba el Informe y lo presenta al Contralor Interno.
5. Una vez revisado y aprobado por el Contralor Interno, se emite el Informe Final, firmado por Contralor Interno, el que será dirigido al Rector de la Universidad de Valparaíso con copia a la (H) Junta Directiva y, en caso de corresponder, a la Unidad auditada.
6. Finalmente, el Informe se deberá escanear y publicar en sitio Web de Contraloría Interna.

Monitoreo de Auditorías TI de la Contraloría General de la República.

1. La Contraloría General de la República audita los procesos relativos a las TI, a nivel de los procesos centrales de la Universidad, detectando hallazgos y riesgos, comunicando los resultados a la Contraloría Interna. En este informe incorpora sus observaciones, hallazgos y recomendaciones en relación al nivel de cumplimiento de la Universidad con las reglamentaciones vigentes asociadas al uso y desarrollo de las TICs.
2. La DISICO desarrolla los planes de acción con el objetivo de mitigar los hallazgos detectados.
3. El Auditor TI asignará valor a la ponderación de probabilidad e impacto de los riesgos detectados por la Contraloría General.
4. Los planes de acción son presentados al Comité de Administración de Riesgos para su aprobación.
5. Una vez que el Comité de Administración de Riesgos aprueba el plan de acción, la Contraloría Interna realizará inspecciones con periodicidad mensual con el objeto de verificar el grado de cumplimiento de los planes de acción definidos.

CONTROLADA

6. El Auditor TI entregará un informe con la actividad de seguimiento realizada, el cual será entregado al Jefe de Control de Gestión Institucional para su validación.

7. El Jefe de Control de Gestión Institucional aprobará el informe y lo entregará al Contralor para ser informado a la Junta Directiva y al Comité de Administración de Riesgos.

Monitoreo de Auditorías TI de Empresas Externas.

1. La Empresa Externa audita los procesos relativos a las TI, detectando hallazgos y riesgos, comunicando los resultados a la Contraloría Interna. En este informe incorpora sus observaciones, hallazgos y recomendaciones en relación al nivel de cumplimiento de la Universidad con las buenas prácticas y con las políticas internas de la Universidad.

2. La DISICO desarrolla los planes de acción con el objetivo de mitigar los hallazgos detectados.

3. El Auditor TI asignará valor a la ponderación de probabilidad e impacto de los riesgos detectados por las Empresas Externas.

4. Los planes de acción son presentados al Comisión de Administración de Riesgos para su aprobación.

5. Una vez que el Comité de Administración de Riesgos aprueba el plan de acción, la Contraloría Interna realizará inspecciones con periodicidad mensual con el objeto de verificar el grado de cumplimiento de los planes de acción definidos. Esta actividad será realiza de manera simultánea con el seguimiento de los planes de acción asociado a los hallazgos de la Contraloría General de la República (procedimiento "PNT-AUDITORIAS TI CGR").

6. El Auditor TI entregará un informe con la actividad de seguimiento realizada, el cual será entregado al Jefe de Control de Gestión Institucional para su validación.

7. El Jefe de Control de Gestión Institucional aprobará el informe de seguimiento mensual, y lo entregará al Contralor para ser informado a la Junta Directiva y al Comité de Administración de Riesgos.

Auditorías TI para Resguardo Patrimonial.

1. El Auditor de Resguardo Patrimonial es el encargado de planificar las actividades relacionadas con los proyectos y procesos Institucionales relacionadas con el resguardo patrimonial. Para ello, solicitará al Auditor TI la planificación de las actividades relacionadas con resguardo patrimonial de las TI.

V°B° CONTRALOR

2. El Auditor de Resguardo Patrimonial entrega al Auditor TI la descripción de la problemática a auditar. Esto incluye, los antecedentes del proceso de negocio sujeto a análisis, la identificación de los riesgos o hallazgos detectados, hipótesis de vulnerabilidades y puntos de interés para los análisis de las TI.

3. El Auditor de Resguardo Patrimonial solicitará al Jefe de Control de Gestión Institucional, en base a los antecedentes de los puntos anteriores, el V°B° para la realización de la Auditoría por parte del Auditor TI.

4. EL Jefe de Control de Gestión Institucional evalúa la necesidad de realizar la Auditoría solicitada, y solicita al Auditor TI que evalúe en base a las prioridades existentes, la factibilidad de su realización, para ello asigna la prioridad de la Auditoría.

5. El Auditor TI informará al Jefe de Control de Gestión Institucional, la factibilidad y plazos de realización de la Auditoría de acuerdo a la prioridad definida.

6. El Jefe de Control de Gestión Institucional da el V°B° para la realización de la Auditoría. Si esto no ocurre la auditoría no se realiza,

7. El Auditor TI planificará a nivel de detalle las actividades de cada auditoría, y será el encargado de ejecutar las pruebas de auditoría, con el fin de verificar y realizar conclusiones técnicas sobre las hipótesis existentes. A su vez, en base a sus propios análisis podrá desarrollar nuevas hipótesis para ser verificadas en las pruebas de auditoría.

8. El Auditor TI en base al procedimiento definido para la realización de pruebas de auditoría (PNTO-PRUEBAS DE AUDITORIA), diseñará y ejecutará las pruebas sobre los sistemas computacionales de la Universidad. A su vez realizará los peritajes requeridos para verificar las hipótesis planteadas, con el fin de verificar sus vulnerabilidades.

9. El Auditor TI en base a los hallazgos detectados durante la Auditoría entregará sus conclusiones técnicas al auditor de Resguardo Patrimonial quien determinará los riesgos existentes en relación al resguardo patrimonial de las TI.

10. El Auditor TI realizará el informe final de la Auditoría, en el cual incluirá el detalle de las pruebas realizadas y los argumentos técnicos que avalan las conclusiones respecto de cada hallazgo.

11. El Auditor TI identificará los Riesgos asociados a sus hallazgos, con su probabilidad e impacto, apoyando al Auditor de Resguardo Patrimonial en la confección de sus matrices de Riesgo, en relación de los temas de TI.

V°B° CONTRALOR

12. El Auditor de Resguardo Patrimonial en base a los antecedentes entregados por el Auditor TI, podría solicitar nuevos peritajes, volviendo al punto 1 de este procedimiento.

13. El Auditor de Fraude incluirá íntegramente los contenidos del informe del Auditor TI en el informe final de la Auditoría. En base a los antecedentes entregados por el Auditor TI y otros análisis realizados por el equipo de Auditores será el encargado de sancionar respecto de los hallazgos que correspondan a Resguardo Patrimonial.

Pruebas de Auditoría TI solicitadas por Auditores Internos

1. El Auditor Interno entrega al Auditor TI la descripción formal de su requerimiento. Esto incluye, los antecedentes del proceso de negocio sujeto a análisis, la identificación de los riesgos o hallazgos detectados, hipótesis de vulnerabilidades y puntos de interés para los análisis de TI.

2. El Auditor interno solicitará al Jefe de Control de Gestión Institucional, en base a los antecedentes de los puntos anteriores, el V°B° para la realización de la Auditoría por parte del Auditor TI.

3. EL Jefe de Control de Gestión Institucional evalúa la necesidad de realizar la Auditoría solicitada, y solicita al Auditor TI que evalúe en base a las prioridades existentes, la factibilidad de su realización, para ello asigna la prioridad de la Auditoría.

4. El Auditor TI informará al Jefe de Control de Gestión Institucional, la factibilidad y plazos de realización de la Auditoría de acuerdo a la prioridad definida.

5. El Jefe de Control de Gestión Institucional da el V°B° para la realización de la Auditoría. Si esto no ocurre la auditoría no se realiza,

6. El Auditor TI planificará a nivel de detalle las actividades de cada auditoría, y será el encargado de ejecutar las pruebas de auditoría, con el fin de verificar y realizar conclusiones técnicas sobre las hipótesis existentes. A su vez, en base a sus propios análisis podrá desarrollar nuevas hipótesis para ser verificadas en las pruebas de auditoría.

7. El Auditor TI en base al procedimiento definido para la realización de pruebas de auditoría (PNTO-PRUEBAS DE AUDITORIA), diseñará y ejecutará las pruebas sobre los sistemas computacionales de la Universidad. A su vez realizará los peritajes requeridos para verificar las hipótesis planteadas, con el fin de verificar sus vulnerabilidades.

COPIA CONTROLADA

8. El Auditor TI en base a los hallazgos detectados durante la Auditoría entregará sus conclusiones técnicas al Auditor Interno para su posterior análisis.

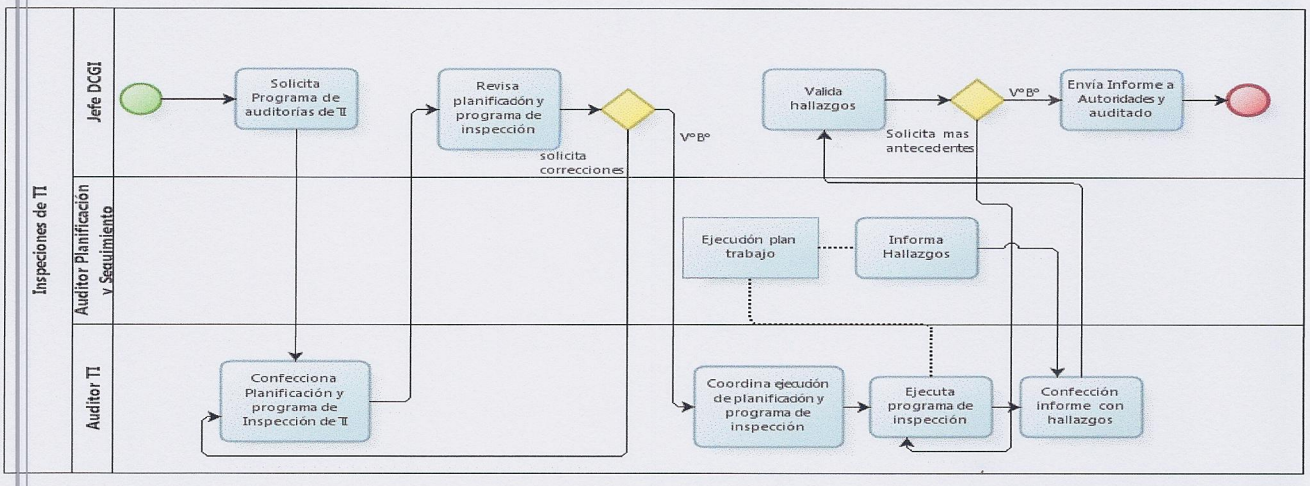
9. El Auditor TI realizará el informe final de la Auditoría, en el cual incluirá el detalle de las pruebas realizadas y los argumentos técnicos que avalan las conclusiones respecto de cada hallazgo.

10. El Auditor TI identificará los Riesgos asociados a sus hallazgos, con su probabilidad e impacto, apoyando al Auditor Interno en la confección de sus matrices de Riesgo, en relación de los temas de TI.

11. El Auditor Interno en base a los antecedentes entregados por el Auditor TI, podría solicitar nuevos peritajes, volviendo al punto 1 de este procedimiento.

12. El Auditor Interno incluirá íntegramente los contenidos del informe del Auditor TI en el informe final de la Auditoría. En base a los antecedentes entregados por el Auditor TI y otros análisis realizados por el equipo de Auditores será el encargado de sancionar respecto de los hallazgos que correspondan a la auditoría.

DESCRIPCIÓN DEL FLUJO (Diagrama)



Powered by bizagi Modeler

V°B° CONTRALOR

INDICADORES PRINCIPALES

Tiempo entre levantamiento del procesos y confección de Matriz de Riesgo.

Tiempo entre envío de Matriz de Riesgo y el Tratamiento de los riesgos identificados.

PUNTOS DE CONTROL

Posterior a la validación, comprobando aprobación.

CONTROL DE MODIFICACIONES

Autor	Fecha	Modificación
Fernando Ríos B.	11/06/2012	Versión 1.0
Fernando Rìos B.	13/09/2012	Unificación de procedimientos de Auditoría TI en este documento.
Fernando Rìos B.	08/10/2012	Corrección de observaciones del Sr. Juan Farías.

COPIA CONTROLADA

V°B° CONTRALOR