UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

Propuesta de un plan para mejorar la gestión de la seguridad informática en los centros desconcentrados de soporte de la Universidad Técnica Nacional Sede Pacifico.

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios del Posgrado en Administración y Dirección de Empresas para optar al grado de **Maestría Profesional en Auditoría de Tecnologías de Información**

SUSTENTANTE:

Javier Antonio Hernández González

Ciudad Universitaria “Rodrigo Facio”, Costa Rica
Julio 2018

DEDICATORIA

Dedico este trabajo de tesis principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mi adorada hija Brithaly Jimena Hernández Molina, que ha sido mi mayor motivación para superarme y para nunca rendirme en los estudios y poder llegar a ser un ejemplo para ella, por ello con todo mi corazón se la dedico con el deseo de que se inspire en mi esfuerzo y llegue a ser grandes cosas en la vida.

A mis padres, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar nuestras di ferencias de opiniones y porque a pesar de nuestra distancia física, siempre están conmigo.

AGRADECIMIENTOS

Gracias a Dios por darme el conocimiento y capacidad para poder comprender cada una de las enseñanzas ofrecidas por los docentes, por proveerme la dicha de despertar cada día, por la diversión vivida a cada momento y sobre todo gracias por haber conocido a toda esa gente excelente a lo largo de la carrera.

Gracias a mi familia por toda la ayuda brindada, por cada una de las palmadas de apoyo ofrecidas, por las preocupaciones, por los regaños, por tener tiempo para oírme, aunque no entendieran de lo que les estaba hablando, por los consejos para continuar adelante.

A mis, amigos, conocidos, a los profesores y a los compañeros por hacerme ver que los limites se los pone uno mismo, por apoyarme a no abandonar mis sueños por enseñarme que las cosas se deben hacer lo mejor posible.

Gracias a los profesores por todas las enseñanzas otorgadas, por clases que nos impartieron, por el apoyo y la confianza para realizar la presente tesis, y porque contribuyeron para lográramos este logro.

Gracias a todos aquellos que no están aquí, pero que me ayudaron a que este gran esfuerzo se volviera realidad.

HOJA DE APROBACIÓN (Proyecto Final)

"Este trabajo final de investigación aplicada fue aceptado por lo Comisión de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial paro optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información."

_____

M.Sc. Gino Ramírez Solís

Profesor del curso

_____

M.Sc. Wendy Vargas Hernández (Profesora UCR)

Tutora (Profesor de Posgrado)

_____

Ing. Wilmer Vindas

Representante Empresa: (Lector)

_____

M.Sc. Ridiguer Artavia Barboza

Director Programa de Posgrado en Administración y Dirección de Empresas

_____

Javier Antonio Hernández González

Sustentante

RESUMEN EN ESPAÑOL

El siguiente proyecto tiene como propósito mejorar la gestión de la seguridad informática en los centros desconcentrados de soporte de la Universidad Técnica Nacional Sede Pacifico mediante la evaluación y promoción del cumplimiento de la normativa desarrollada por la institución, contenida y aprobada por la Comisión Institucional de Gestión Informática en 2016, y aplicable en la gestión de la seguridad del departamento de coordinación de TI en las áreas de: mantenimiento, gestión de proyectos y soporte técnico.

Por medio del desarrollo de un análisis de la normativa y estándares institucionales establecidos para la gestión de la seguridad de tecnologías de información por el departamento de soporte de TI de la Sede del Pacífico de la Universidad Técnica Nacional, y su comparación con las utilizadas por el Departamento de Coordinación de TI de Sede, se identificaron condiciones que deben ser mejoradas para lo cual se propone un "plan para el mejoramiento la gestión de la seguridad en materia de tecnologías de información en los centros de soporte de las sede Pacífico de la Universidad Técnica Nacional".

Durante el desarrollo del trabajo se logró determinar las siguientes causas de incumplimientos de la normativa:

- A la fecha de este análisis, la Sede Pacífico no cuenta con personal en el área de seguridad, por lo que procedimientos críticos no son llevados a cabo, excepto por algunas tareas a cargo del Coordinador de TI de la sede.
- La falta de definir en los procedimientos personas responsables de realizar las tareas indicadas en dicha normativa.
- La falta de la desactivación de cuentas de personal que han finalizado en forma temporal o permanente su relación contractual con la Universidad.
- El desconocimiento de los funcionarios en lo a temas de seguridad de información se refiere.

Para dar solución a dichas causas se recomendó:

- Presupuestar y ejecutar lo necesario, para contar con el personal de Seguridad de la Información que debe cumplir con la Normativa de TI 1.4. Gestión de la Seguridad de la Información.
- Tomar las acciones necesarias para asegurar el control del software instalado, las adquisiciones de hardware y software para la sede del Pacífico, como son la ejecución de revisiones periódica, y la verificación del equipo instalado acorde con lo establecido en el Manual de Estándares de Equipo de TI.
- Contar con inventarios actualizados de la infraestructura tecnológica institucional de forma que se controle los activos asociados a la Seguridad de la información.
- Realizar una evaluación de los perfiles de los usuarios que tienen asignada una contraseña y determinar, según la necesidad de uso, los horarios y acceso que deben tener vigentes a cada perfil

ABSTRACT

Through the development of the following project, we sought to improve the management of information security in the deconcentrated centers of support of the Universidad Técnica Nacional Sede Pacífico by applying the regulations developed by the institution, contained and approved by the Institutional Management Commission in 2016., through the identification and evaluation of the guidelines and standards currently applied in the security management of the IT coordination department in the areas of: maintenance, project management and technical support.

Through the development of an analysis of the regulations and institutional standards of information technology security management in the IT support department of the Pacific Headquarters of the National Technical University, a comparison and evaluation was carried out against those used by the Headquarters IT coordination department in such a way that improvements and updates were identified and a plan for the improvement of security management in information technology at the National Technical University was proposed.

During the development of the work it was possible to determine the following causes that make it impossible for the regulation to be applied:

- The Institution does not have personnel in the security area yet, so the above procedures are not carried out by said personnel, but rather by the IT Coordinator of the headquarters.
- The lack of defining in the procedures persons responsible for carrying out the tasks indicated in said regulations.
- The lack of deactivation of personnel accounts that have temporarily or permanently completed their contractual relationship with the University.
- The lack of knowledge on the part of officials regarding information security matters.

To solve these causes, it was recommended:

- Budget and execute what is necessary to have the Information Security personnel that must comply with the IT Regulations 1.4. Information Security Management.
- Take the necessary actions to ensure control of the installed software, hardware and software purchases for the Pacific headquarters, such as the execution of periodic reviews, and the verification of the equipment installed in accordance with the provisions of the Equipment Standards Manual of you.
- Have up-to-date inventories of the institutional technological infrastructure in order to control the assets associated with Information Security.
- Carry out an evaluation of the profiles of the users who have assigned a password and determine, according to the need to use, the schedules and access that must be valid for each profile.

TABLA DE CONTENIDOS

NOMENCLATURA

Nemónico	Definición
DGTI	Dirección de Gestión de Tecnologías de Información
TI	Tecnologías de Información
PETIC	Plan Estratégico de Tecnología Informática y Comunicaciones
PTAC	plan táctico en tecnologías de Información y comunicación
BD	Base de datos
TFG	Trabajo Final de Graduación
UCR	Universidad de Costa Rica
CGR	Contraloría General de la República
NIA	Normas Internacionales de Auditoría
DGTI	Dirección de Gestión de Tecnologías de Información
CUNA	Colegio Universitario de Alajuela
CUP	Colegio Universitario de Puntarenas
CURDTS	Colegio Universitario para el Riego y Desarrollo del Trópico Seco
ECAG	Escuela Centroamérica de Ganadería
CIPET	Centro de Investigación y Perfeccionamiento para la Educación Técnica
CEFOF	Centro de Formación de Formadores y de Personal Técnico para el Desarrollo Industrial de Centroamérica.
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas
TICs	Tecnologías de la Información y la Comunicación

INTRODUCCIÓN

El presente documento nombrado " Propuesta de un plan para mejorar la gestión de la seguridad informática en los centros desconcentrados de soporte de Universidad Técnica Nacional Sede Pacifico "ha sido elaborado como trabajo de tesis previa la obtención del título Maestría Profesional en Auditoría de Tecnologías de Información en Universidad de Costa Rica. En dichos proyectos se estableció como objetivo general de lograr mejoras significativas en la gestión de la seguridad informática en los centros desconcentrados de La Universidad Técnica Nacional, mediante la evaluación de la normativa Institucional.

De acuerdo a los objetivos específicos, el proyecto marca su inicio realizando la identificación y evaluación, y análisis de los lineamientos actuales y estándares aplicados a la gestión de seguridad en la sede pacifico, para posteriormente realizar un informe que determine si cada uno de los procesos de TI colaboran competentemente con la consecución de los objetivos de la normativa, precisando a realizar un conjunto de recomendaciones en base a los resultados obtenidos de dicha evaluación.

Como bien se sabe la evaluación de que las políticas y procedimientos establecidos, y la aplicación de estas de manera oportuna y eficiente permitirá un mejoramiento continuo, además de proveer de fortalecimiento tecnológico, que brinde soporte efectivo a sus operaciones de control de los servicios de la institución.

El presente trabajo no tiene como finalidad descubrir errores y marcar fallas, sino más bien permitirá fortalecer debilidades y mejorar la aportación de las TICs a la

consecución de los objetivos institucionales de la UTN, mediante recomendaciones.

JUSTIFICACIÓN

Se sabe que la seguridad informática en estos años es una necesidad para cualquier institución y para ello contar con protocolos, controles, procedimientos, normativas, directrices, manuales, reglamentos y que el cumplimiento de estos, permiten que se cumpla con los objetivos de forma satisfactoria, como son el mantener la continuidad de los servicios ofrecidos por las empresas o instituciones, confidencialidad y seguridad de la información; conservando intacta las características principales con que debe contar la información, de forma lograr los objetivo de asegurar que los equipos, materiales, productos, procesos y servicios que desarrollan las instituciones o empresas.

Por este motivo esta propuesta es la base para que la institución cumpla con todos los controles elaborados y diseñados, para ser aplicados en la sede en cuestión y en las demás sedes, de modo que se cuenta con la protección necesaria y una adecuada seguridad de los activos de información.

Actualmente la institución posee una infraestructura tecnológica en desarrollo de la cual dependen tanto el área administrativa como el área docente, y mucha de la información que procesan se encuentra en los equipos, servidores de archivos, correos electrónicos, información en físico almacenada en archivadores, y otros en sistemas de almacenamiento de información ya sean discos duros externos, Discos compactos (CD), Disco Versátiles Digitales (DVD), bases de datos etc.

La institución cuenta además con políticas de seguridad para resguardar tanto equipos informáticos como información, así también cuenta con una estructura institucional y con el equipo y la tecnología necesarias para desarrollarlas, pero muchas de estas políticas no están siendo aplicadas en las diferentes Sedes, como institución en miras de vanguardia en la educación surge la necesidad de alinear los objetivos de ti para lograr alcanzar los objetivos institucionales basados en dichas políticas, en el PETIC y en el PETAC de TI, en directrices nacionales e internacionales ; para ellos es necesario iniciar con una auditoría para verificar los puntos que la institución debe fortalecer, para alcanzar las metas y objetivos fijados y de esta manera cumplir con lo que solicitó la Contraloría General de la República.

Por medio de esta evaluación se quiere lograr agregar valor y mejorar las operaciones de TI y a su vez de la institución. De modo de lograr ayudar a cumplir sus objetivos, aportando un enfoque sistemático y disciplinado para evaluar y mejorar el cumplimiento de la normativa institucional en materia de Tecnologías aprobada por la Comisión institucional de Gestión Informática.

Al final se plantean las conclusiones mediante la evaluación mencionada brindando las recomendaciones para aplicar como estrategia para la administración de la seguridad en los departamentos de las sedes.

Ingresar el análisis que se realizará está basado en documentos de la institución relacionados con el tema, de las diferentes fuentes para sustentar el marco teórico y la vivencia propia del autor en su trabajo diario en la sede.

OBJETIVOS

1. OBJETIVO GENERAL

Lograr mejoras significativas en la gestión de la seguridad informática en uno de los centros desconcentrados de soporte informático un centro universitario público, por medio de una evaluación de la normativa Institucional, contenida y aprobada por la Comisión institucional de Gestión Informática en 2016.

2. OBJETIVOS ESPECÍFICOS.

1. Identificar y evaluar los lineamientos y estándares aplicados actualmente en la gestión de la seguridad del departamento de coordinación de TI en las áreas de: mantenimiento, gestión de proyectos y soporte técnico.

2. Analizar la normativa y estándares institucionales de la gestión de la seguridad de tecnologías de información en el departamento de soporte de TI de la Sede del Pacífico de la Universidad Técnica Nacional, contenida y aprobada por la Comisión Institucional de Gestión Informática en el 2016, con el fin de realizar una comparación contra las utilizadas por el departamento de coordinación de TI.

3. Evaluar políticas utilizadas en la Sede del Pacífico en cuanto a la gestión de la seguridad a fin de identificar eventuales mejoras y actualizaciones.

4. Proponer un plan para el mejoramiento la gestión de la seguridad en materia de tecnologías de información en la Universidad Técnica Nacional

ALCANCE DEL PROYECTO

El presente trabajo final de graduación llamado: Propuesta de un plan para mejorar la gestión de la seguridad informática en los centros desconcentrados de soporte de Universidad Técnica Nacional Sede Pacifico, Como parte de este proyecto se identificarán las normas aplicables a la gestión de la seguridad de los Deptos. De Coordinación de TI de la Sede Pacífico, y su implementación en los diferentes procesos que realizan. El periodo de examen comprende del 1 de enero 2018 al 31 de marzo del mismo año.

Como criterio principal se considerarán las normas dictada en el año 2016 por la Comisión Institucional de Gestión Informática.

LIMITACIONES

El proyecto será desarrollado en la Universidad Técnica Nacional en la Sede Pacífico y su alcance evaluará la aplicación al cumplimiento de la Normativa de TI en lo que corresponde a gestión de la seguridad de la información.

Debido al tiempo con que se cuenta a para su ejecución no es posible efectuar un estudio a nivel general que abarque a todas las sedes.

MARCO METODOLÓGICO

2.1.1. Clasificación de la investigación

El presente trabajo, según Barrantes Echavarría, 1999 se clasifica de la siguiente manera:

Se considera una investigación aplicada, ya que se aplica el conocimiento adquirido durante la maestría a un caso real en una empresa costarricense, con la finalidad de detectar

los procesos y elementos críticos mediante la aplicación de la normativa creada en la institución. El estudio realizado no pretende aportar un conocimiento teórico nuevo al campo de la Continuidad del negocio sino atacar potenciales problemas generadores de riesgo para la continuidad del negocio evaluado.

Respecto a su alcance temporal, es una investigación transversal o sincrónica, ya que se realiza en un momento dado (noviembre 2017 hasta abril 2018) y los datos o situaciones analizadas también pertenecen a este mismo período.

Según su profundidad u objeto, se puede catalogar como descriptiva, ya que describe una condición encontrada, que se valora contra unos criterios normativos establecidos que rigen el tema evaluado tanto a nivel interno como externo.

En su enfoque o medición, se considera cualitativa, ya que se describirán situaciones de los procesos de la empresa evaluada sin cuantificar o manipular datos numéricos específicos, más que los que se observan o responden en instrumentos cualitativos. Tiene lugar en el campo y no en un laboratorio, con situaciones naturales y libertad de acción de los observados.

La validez de la investigación radica la evidencia que recaba el postulante durante su trabajo de campo y el debido proceso de ejecución. La confiabilidad se ampara en el diseño de los instrumentos denominados como “Papeles de Trabajo” que se basan en la normativa (interna y externa), estándares, criterio experto y mejores prácticas en el campo evaluado.

2.1.2. Aproximación al marco metodológico e instrumentos a utilizar

Para iniciar con el marco metodológico se considera pertinente definir los siguientes dos conceptos:

- **Método:** manera de ordenar una actividad, orden sistemático que se impone en la investigación, camino para llegar a cierto resultado, que se compone de varias técnicas. (Barrantes Echavarría, 1999, págs. 48-60)

- **Técnica:** es un conjunto de instrumentos de medición, elaborados con base en los conocimientos, mismas que pueden ser de medición o de recolección de la información (Barrantes Echavarría, 1999, págs. 60-61)

Considerando que la institución donde se realiza el trabajo a pesar de ser autónoma pertenece al sector público y en la cual se estará realizando la evaluación de la norma, aunado a que existe un ente rector) que norma la metodología para realizar auditorías mediante el documento "Normas generales de Auditoría para Sector Público" (CGR, 2014), que son de acatamiento obligatorio para el Sector Público y prevalecen sobre cualquier disposición en contrario que emitan otros órganos competentes, se adaptarán las normas 203-204-205 y 207.este marco como método del presente trabajo de la siguiente manera:

Norma 203. Planificación (Contraloría General de la República, 2014, págs. 6-8)

La evaluación de la Norma de DGTI de la sede del Pacífico se planificará de forma que garantice la realización de una labor de alta calidad de un modo económico, eficiente y eficaz y de manera auditoría oportuna (momento) y de acuerdo con los principios de la buena gestión de proyectos.

La evaluación de la aplicación de la norma debe permitir un uso eficiente de los recursos involucrados y se puedan incorporar los ajustes que correspondan durante su desarrollo. Para lo anterior se debe tener claro el objetivo, naturaleza, alcance, oportunidad y plazo para llevar a cabo el trabajo en el tiempo establecido. Además, debe obtener un conocimiento de la entidad, la comprensión del sistema de control interno relacionado con el asunto objeto de auditoría, así como la identificación de los criterios de auditoría que serán aplicados.

Con los insumos de información y conocimiento, se realizará una evaluación del riesgo, que conduzca a seleccionar las áreas a auditar en la actividad de examen y permitirá la elaboración del Programa de Auditoría.

En la actividad de planificación se debe preparar y aprobar el programa específico que el postulante elaboró, para ser ejecutado durante la actividad de examen

Instrumentos diseñados en esta etapa

- **Cuestionarios.** Al personal encargado de la gestión de TI, a usuarios respecto a su percepción de la gestión de TI y cualquier otro personal de interés.
- **Plantillas de trabajo.** Papeles de trabajo para evaluar o describir condiciones encontradas, listas de chequeo, cuadros resúmenes de información recopilada, resultados de pruebas, hojas de recolección de hallazgos, etc.
- **Guías de entrevistas.** Al personal encargado de la gestión de TI, a los entes rectores de emitir y aprobar la normativa interna en esta materia (jefe de TI y Comisión institucional de Gestión Informática), a usuarios respecto a su percepción de la gestión de TI y cualquier otro personal de interés.
- **Mapa o Cuadro de Riesgo.** El mapa o cuadro de riesgos es una herramienta que tiene por objeto mostrar gráficamente el diagnóstico del proceso de evaluación de riesgos que se identificaron en esta etapa de Planificación. Se determina mediante la interacción de la probabilidad o frecuencia por el impacto de los tipos de riesgos en los diferentes procesos, actividades o funciones de un negocio.
- **Programa de trabajo.** Es un documento formal que se utiliza como guía metodológica en la realización del trabajo. El programa indica la descripción de actividades a desarrollar de acuerdo a un orden y una lógica, y dentro de un periodo o tiempo determinado.

Norma 204. Examen o trabajo de campo (Contraloría General de la República, 2014, pág. 8)

Durante la actividad de examen se debe ejecutar el programa realizado en la etapa de planificación. Se ejecuta en forma ordenada las actividades dispuestas, lo cual conlleva a realizar pruebas, evaluar controles y recolectar la evidencia necesaria mediante la

utilización de técnicas y prácticas de auditoría para determinar, justificar y presentar apropiadamente los hallazgos de auditoría, con sus atributos de criterio, condición, causa y efecto.

Se aplican todos los papeles de trabajo diseñados en la etapa de planificación y cualquier otro requerido de acuerdo a los hallazgos encontrados, todo siguiendo el debido proceso tanto de la ejecución como en la recolección de evidencia; se verifica la calidad y trazabilidad desde el programa de trabajo hasta el último papel de trabajo diseñado y aplicado.

Instrumentos aplicados en esta etapa

- **Cuestionarios.** Al personal encargado de la gestión de TI, a usuarios respecto a su percepción de la gestión de TI y cualquier otro personal de interés.
- **Plantillas de trabajo.** Papeles de trabajo para evaluar o describir condiciones encontradas, listas de chequeo, cuadros resúmenes de información recopilada, resultados de pruebas, etc.
- **Entrevistas.** Aplicadas al personal encargado de la gestión de TI, a los entes rectores de emitir y aprobar la normativa interna en esta materia (jefe de TI y Comisión institucional de Gestión Informática), a usuarios respecto a su percepción de la gestión de TI y cualquier otro personal de interés.
- **Programa de trabajo.** Es un documento formal que se utiliza como guía metodológica en la realización del trabajo. El programa indica la descripción de actividades a desarrollar de acuerdo a un orden y una lógica, y dentro de un periodo o tiempo determinado.
- **Hojas de hallazgos.** Se recolecta todos los hallazgos en la hoja de hallazgos correspondiente. Considerando:

Norma 205**. Comunicación de resultados** (Contraloría General de la República, 2014, págs. 8-9)

Una vez concluido el trabajo de campo y aprobado el Informe Borrador, se comunica a instancias correspondientes de la sede universitaria, sobre los principales resultados, las conclusiones y las recomendaciones producto de la auditoría que se llevó a cabo, lo que constituirá la base para el mejoramiento de los asuntos examinados.

El informe preliminar de auditoría se elabora en un lenguaje sencillo, ser objetivos, concisos, claros, completos, exactos e imparciales, basados en hechos y respaldados con evidencia suficiente, competente y pertinente.

El postulante efectúa una conferencia final con la Administración de la entidad u órgano auditado y con los responsables de poner en práctica las recomendaciones o disposiciones, antes de emitir el Informe Definitivo, con el fin de exponer los resultados, conclusiones y disposiciones o recomendaciones de la auditoría, de conformidad con lo establecido en los objetivos y alcance del proyecto, que ya conocen los interesados.

El informe de auditoría contiene un resumen ejecutivo de los principales resultados obtenidos, así como de las conclusiones, disposiciones o recomendaciones emitidas.

Las recomendaciones contemplan al menos lo siguiente: a) Generar valora la entidad b) Atacar las causas del problema o condición identificada, c) Dirigidas al nivel responsable de solventar la deficiencia y d) Ser claras, específicas, convincentes y relevantes.

Entregables en esta etapa

- **Informe definitivo.** Debe incorporar las observaciones de la administración a cada hallazgo, observación o recomendación, si lo evidenciaron suficiente.
- **Acta de reunión de comunicación de resultados.** Contiene los datos de fecha, hora inicio y fin; participantes convocados y presentes (con firma), observaciones y comentarios con nombre completo y puesto.
- **Recibido conforme de la institución.** Documento emitido por la misma persona que autorizó la realización del evento con firma de persona

contacto (cuando fuese diferente). Indicando el cumplimiento de lo acordado y el grado de satisfacción con el trabajo.

CAPITULO I
PERSPECTIVAS TEÓRICAS

PERSPECTIVAS TEÓRICAS

1.1. Estado de la cuestión en Costa Rica

Como se ha demostrado las autoevaluaciones de las normas de los departamentos de tecnologías de información brinda un valioso aporte el desarrollo, además de que fortalecen las estrategias empresariales logrando el éxito organizacional, tal ha sido su importancia que se hace necesario estimar un modelo que permita valorar su efectividad en este entorno.

Son muy pocos los casos claramente conocidos en Costa Rica como de TI, sin embargo, lo cierto es que la debida aplicación de las normativas adoptadas en los departamentos de TI; en los tiempos actuales en todo fraude financiero hay elementos de tecnología asociados y utilizados como medios para realizar el fraude.

Hasta hace pocos años se empezó a dar el fenómeno de las auditorias de TI, la Universidad de Costa Rica (UCR) ha sido una de las instituciones con la carrera de Maestría que ha presentado trabajos con este tipo de auditorías, enfocándose a la aplicación de la auditoría de Información como el proceso básico para evaluar el estado de la gestión de los recursos de información en las organizaciones, en esta investigación se exponen algunos conceptos de gestión de la información y auditoría de información.

Anterior al auge que han tenido en esta década la Auditoría de TI, la mayoría de los trabajos, publicaciones e investigaciones abarcan temas financieros que no asociaban con el diseño de Sistemas de Información, como un recurso o un activo institucional o sobre la necesidad de administrarlo dicho recurso como tal por ser soporte de toda la gestión sustantiva de las organizaciones, incluidas instituciones educativas como la Universidad Técnica Nacional (UTN).

En nuestro país conforme han ido avanzando las tecnologías hemos experimentado en las instituciones diferentes eventos delictivos como son el duplicado de las páginas de los bancos del estado, robos de dinero mediante skimming, ataques de denegación de servicios, y muchos otros que también se dan a nivel mundial.

Al estar expuesta a todos estos ataques, la Contraloría General de la República establece las Normas técnicas para la gestión y el Control de las Tecnologías de

Información (Contraloría General de la República, 2007, pág. i) la cual instituye los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado y que a su vez es una Directriz vinculante para todas las instituciones públicas del Estado, basados principalmente en COBIT e ITIL, que son estándares internacionales para la gestión de las tecnologías de información y comunicación.

1.2. Historia de la institución donde se desarrollará

La Universidad Técnica Nacional (Universidad Técnica Nacional , 2016, pág. 5) tiene el fin de dar atención a las necesidades de formación científica, técnica y tecnológica que requiere el país, en todos los niveles de educación superior universitaria, que culminen con la obtención de títulos y grados universitarios, con énfasis especial en las carreras técnicas que demanda el desarrollo nacional.

La Universidad Técnica Nacional nace como una nueva opción educativa, con el fin de contribuir a la superación de dos grandes brechas. Por un lado, la separación entre la educación técnica tradicional y la educación universitaria, que, en el caso de Costa Rica, como en casi toda América Latina, constituyen niveles y ámbitos educativos separados, los cuales han carecido de medios de articulación e integración eficaces y fructíferos, de cara a las necesidades del desarrollo. Por el otro lado, la también tradicional ruptura entre la academia universitaria y los sectores productivos, entre las instituciones de educación y el mundo real del trabajo y de la empresa. Por ello, a la Universidad Técnica Nacional se le establecen mandatos específicos y se le otorgan competencias concretas en su ley de creación, con el claro objetivo de que la institución sea un factor activo que pueda contribuir a superar esas brechas.

En esa dirección, y, en primer término, nuestra Ley Orgánica de la Universidad Técnica Nacional (Asamblea Legislativa de la República de Costa Rica, 2008, pág. 2) postula que la Universidad está obligada a desarrollar sus acciones como parte de un esfuerzo para alcanzar el “mejoramiento integral de la sociedad costarricense, el fortalecimiento de su democracia y la creación de condiciones económicas y sociales más equitativas y justas

para la convivencia social, especialmente el fomento de actividades productivas y la generación de empleo".

Para el cumplimiento de ese propósito esencial, la Universidad tiene como fines básicos, entre otros, el de ofrecer a sus estudiantes "una educación integral que les garantice simultáneamente su óptima formación profesional y técnica, así como su desarrollo integral, moral, cultural y personal", sin demérito de que, por su naturaleza específica, la Universidad le debe brindar "énfasis especial a las carreras técnicas que demanda el desarrollo nacional".

En materia de vinculación con el sector productivo, la ley establece el mandato específico de que los programas de investigación de la Universidad, deben coadyuvar en los procesos de desarrollo, modernización y mejoramiento técnico de los sectores productivos, las empresas exportadoras y, especialmente, las pequeñas y medianas empresas. En este campo específico, el del respaldo a las pequeñas empresas, la Universidad está obligada además a "desarrollar programas especiales de fortalecimiento de las pequeñas y medianas empresas, mediante acciones de asistencia técnica, capacitación y formación integral, para procurar su desarrollo y expansión".

Descripción de la Institución

La Universidad Técnica Nacional nació como resultado de la fusión legal de las siguientes instituciones de educación técnica superior (Universidad Técnica Nacional, 2015):

- Colegio Universitario de Alajuela (CUNA).
- Colegio Universitario de Puntarenas (CUP).
- Colegio Universitario para el Riego y Desarrollo del Trópico Seco (CURDTS).
- Escuela Centroamérica de Ganadería (ECAG).
- Centro de Investigación y Perfeccionamiento para la Educación Técnica (CIPET).
- Centro de Formación de Formadores y de Personal Técnico para el Desarrollo Industrial de Centroamérica (CEFOF).

Sede Central

Sede Atenas

Sede del Pacífico

Sede Guanacaste

Sede San Carlos

Todas ellas con una larga experiencia académica y una valiosa trayectoria histórica, lo cual facilitó acelerar el proceso de integración académica inicial de la Universidad, y permitió brindar muy rápidamente una amplia y diversificada oferta educativa.

La Universidad Técnica Nacional surge del convencimiento de que no estábamos preparando a la juventud costarricense, con la celeridad requerida, para los desafíos de la sociedad del conocimiento; ni estábamos garantizando, con la cobertura necesaria, una

transmisión de conocimientos, habilidades y competencias profesionales y ocupacionales adecuados y pertinentes, para que los nuevos contingentes laborales del país se puedan insertar exitosamente en el mundo productivo del futuro, enmarcado en procesos de globalización, apertura comercial y alta competitividad. (Universidad Técnica Nacional, 2013, pág. 11).

En el periodo de nacimiento y desarrollo alcanzó significativos logros en la educación superior para miles de jóvenes costarricenses, repartidos en cinco sedes y un centro especializado.

Ubicación Geográfica

La Universidad Técnica Nacional Sede del Pacífico está ubicada en la provincia de Puntarenas, Recinto Tobías Vargas en Puntarenas Centro: 100 metros al oeste del Muelle de Cruceros sobre el Paseo de los Turistas, frente a la Concha Acústica, en el edificio de la antigua aduana (Universidad Técnica Nacional, 2015)

Cuenta con un edificio de 10.000 m2 donde se llevan a cabo las funciones administrativas y docentes. Mapa satelital de la ubicación geográfica (Universidad Técnica Nacional, 2015).

Además, el Recinto Campus Juan Rafael Mora Porras, inaugurado en enero del año 2011, ubicado en El Roble de Puntarenas; antigua finca Socorrito, 700 metros al norte y 900 al oeste de la entrada principal del Roble, Costado sur del plantel de Coope Roble R.L.

Marco Estratégico Institucional

A continuación, se presentan los componentes del Marco Filosófico y los Ejes Estratégicos de la Universidad Técnica Nacional (Universidad Técnica Nacional, 2015).

Marco Filosófico

De acuerdo con el Plan Estratégico, Sede del Pacífico, 2011, se citarán la Visión, Misión, Valores Institucionales y Políticas Institucionales, pues son pilares fundamentales en la Universidad Técnica Nacional (UTN).

Visión

Ser universidad de vanguardia en la formación integral de profesionales, la investigación y la acción social en las áreas científicas, técnicas y tecnológicas, con un enfoque de humanismo científico innovador, que contribuya al desarrollo sostenible de la sociedad costarricense.

Misión

Brindar una educación integral de excelencia, en el marco de la moderna sociedad del conocimiento, centrando su acción académica en el área científica, técnica y tecnológica, en la investigación de alta calidad y en la innovación como elementos fundamentales para el desarrollo humano con responsabilidad ambiental, en articulación con los sectores productivos de la sociedad.

Objetivos o fines de la Universidad Técnica Nacional:

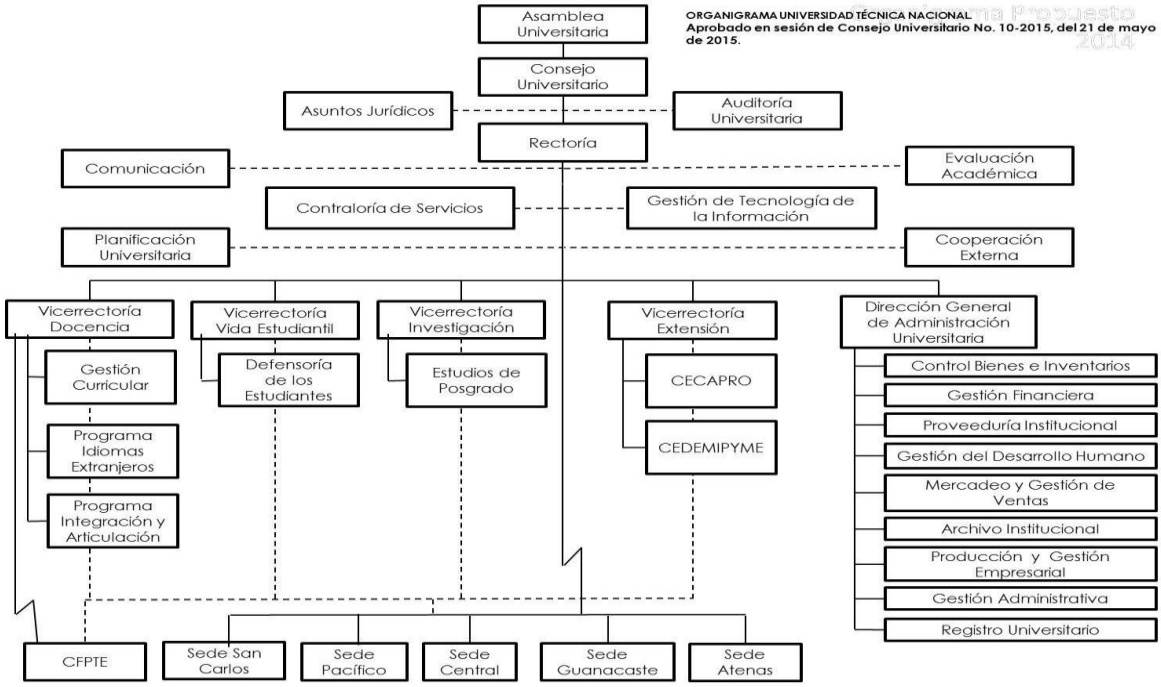
La ley n° 8638 de creación establece como sus fines los siguientes (ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA, 2008):

a) Crear, conservar, transformar y transmitir el conocimiento en el marco de un esfuerzo sostenido, orientado al mejoramiento integral de la sociedad costarricense, al fortalecimiento de su eficiencia, su equidad, su sostenibilidad y su democracia.
b) Ofrecer, a sus estudiantes una educación integral que fomente su óptima formación profesional y técnica, así como su desarrollo personal, ético y cultural.
c) Promover la investigación científica y científico-tecnológica de alto nivel académico, para contribuir al mejoramiento de la vida social, cultural, política y económica del país.
d) Coadyuvar en los procesos de desarrollo, modernización y mejoramiento técnico de los sectores productivos.
e) Preparar profesionales de nivel superior, por medio de carreras universitarias que guarden armonía con los requerimientos científicos y tecnológicos del desarrollo mundial y las necesidades del país, que culminen con la obtención de títulos y grados universitarios, dando énfasis especial a las carreras técnicas que demanda el desarrollo nacional.
f) Desarrollar carreras cortas en el nivel de pregrado universitario, que faculten para el desempeño profesional satisfactorio y la inserción laboral adecuada. Dichas carreras serán parte de las carreras de grado de la Universidad y podrán articularse con los programas de estudio de las especialidades de Educación Técnica Profesional del Ministerio de Educación Pública y con programas Técnicos del Instituto Nacional de

Aprendizaje y cualquier otra opción educativa impartida por un Centro de Educación Superior o Técnica, con garantía, en todo caso, del cumplimiento de los requisitos de la Universidad.

g) Desarrollar programas de formación y capacitación pedagógica para su personal académico, sus egresados y los de otras instituciones de educación superior.
h) Desarrollar programas especiales para la formación y fortalecimiento del micro, pequeñas y medianas empresas.

Estructura Organizacional



Historia del Departamento de TI

Los departamentos de TI ya existían en cada uno de las instituciones fusionadas, en el 2010 el rector, conforma la Comisión Institucional de Informática integrada por los responsables de las unidades de informática de cada Sede o Centro el oficio R-367-2010 (UNIVERSIDAD TÉCNICA NACIONAL, 2010) (Contraloría General de la República, 2013), la cual según Informe de Auditoría No. 07 de la Contraloría General de la Republica (CGR), no cumplía con el requisito de contar con representación de todas las áreas

involucradas en la gestión informática de la Universidad, y tenía simples y limitadas funciones de coordinación, que el Director de Informática le falta la asignación de autoridad técnica formal sobre las Unidades de Informática de la Sedes y Centro de Formación; y que además los jefes/encargados de las Unidades de Informática no tienen la obligación de consultar con el Director de Informática los proyectos o inversiones de TI, que se realizan en las Sedes.

Por lo que la CGR recomendó que se debe tener representación de todas las áreas o direcciones estratégicas de la Universidad y a la vez debe ser liderada por el señor Rector; para garantizar que las decisiones que tome el equipo implementador tenga la autoridad suficiente, el respeto y colaboración inmediata de todas las áreas de la Universidad y a la vez se consideren los puntos de vistas de todas las áreas estratégicas de la Universidad, para así lograr alinear las Tecnologías de la Información a los Objetivos Estratégicos de la Institución y que el Director de Informática de la UTN, se le asigne la autoridad técnica correspondiente con respecto a los Jefes/encargados de las Unidades de Informática de las Sedes y Centro de Formación, con el fin de poder desarrollar y coordinar de forma fluida los proyectos de tecnologías de la institucionales (Contraloría General de la República, 2013)

Luego en el periodo 2014-2015 se creará la Dirección de Gestión de Tecnologías de la Información (DGTI) para cumplir con sus objetivos, siendo la encargada de la dirección estratégica de Tecnología Informática y Comunicación de la UTN, cuya función es la de dirigir y administrar los recursos de tecnologías de información de la Universidad, garantizando la alineación con los objetivos estratégicos Institucionales, con el objeto de proporcionar las herramientas necesarias para realizar en forma eficiente las funciones administrativas y sustantivas que requiere la Institución, lo cual se logra mediante la definición y aplicación de normas y procedimientos tanto en materia de servicios e infraestructura como en sistemas institucionales, esta será asesorada por un Comité Asesor Técnico (CAT) y por un Gestor de Seguimiento y Control de TI (Universidad Técnica Nacional, 2016).

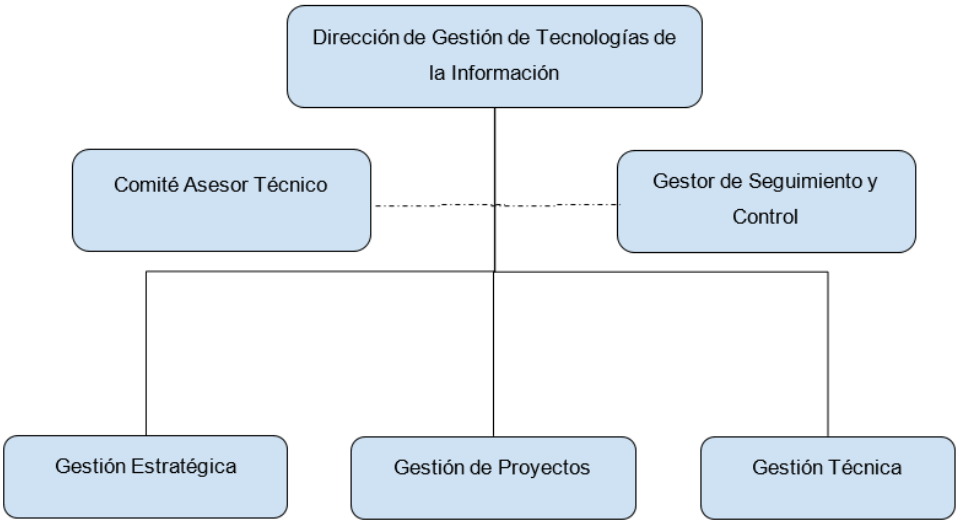
Comité Asesor Técnico (CAT): apoya al Director de TI en el desarrollo de la Tecnología dentro de la Universidad, coordina su aplicación, da seguimiento y evalúa las

acciones derivadas del mismo, conformado por los Jefes de área, los acuerdos que tomados por dicho el comité podrán ser aplicados por la Dirección.

Gestor de Seguimiento y Control de TI: tiene como función planear, organizar, coordinar, supervisar, ejecutar, controlar y evaluar labores técnicas, profesionales y administrativas. Además de brindar asesoría a la DGTI con el fin de garantizar el cumplimiento de los Objetivos de TI universitarios, además del control de las actividades relacionadas con el sistema de evaluación del riesgo y los planes de mejoras.

Para desarrollar sus objetivos la Dirección contará con el aporte de tres Áreas con funciones ejecutivas que gestionará las TIC institucionales, las cuales son: **Gestión Estratégica, Gestión de Proyectos y Gestión Técnica.**

FIGURA Nº 1 ORGANIGRAMA DGTI



(Universidad Técnica Nacional, 2016)

Misión

- Liderar la gestión de las tecnologías de la información y la comunicación en la Universidad, brindando con alta calidad e innovación los productos y servicios requeridos por la comunidad universitaria.

Visión

- Ser el ente institucional en el campo de las tecnologías de la información y la comunicación, que potencien y orienten a la universidad hacia una posición de vanguardia y excelencia a nivel nacional en los campos de la docencia, extensión, investigación, innovación, vida estudiantil y administración.

Objetivos Estratégicos de DGTI

- Disponer de los recursos TIC requeridos por la comunidad universitaria, mediante acciones específicas de mejoramiento técnico, operativo y tecnológico que permitan el adecuado desarrollo universitario.
- Desarrollar proyectos TIC enfocados en el mejoramiento y desarrollo de los procesos estratégicos institucionales.
- Desarrollar un plan de recursos humanos técnicos y profesionales que permitan el desarrollo del área de TI en la Universidad.
- Establecer mecanismos de rendición de cuentas y alfabetización digital que permita a la Institución posicionarse ante la sociedad, los sectores productivos y el sistema universitario.
- Desarrollar un programa ambiental que permita la disposición de desechos y aprovechamiento de recursos de corte tecnológico en función de las necesidades institucionales.
- Desarrollar un programa de información oportuna, confiable y veraz de nivel institucional, mediante el aprovechamiento de las TIC en función de las necesidades de la organización.
- Gestionar en forma continua y eficiente el Marco de Gestión de Riesgos de TI de la Universidad.
- Cumplir con leyes, reglamentos, normas y otros, sobre el uso y adquisición de tecnologías informáticas y de telecomunicaciones.
- Administrar eficientemente los recursos económicos asignados por la Universidad.

1.3. Normativa asociada

Como resultado de la auditoría realizada por la contraloría según informe N° DFOE-SOC-IF-12-2013, del 19 de noviembre, 2013 (Contraloría General de la República, 2013), la institución no contaba con una estructura orgánica integrada, flexible y funcional, conforme a las necesidades de la institución, además de la escasa existencia de una normativa básica, ni planes de contingencia para el funcionamiento de las tecnologías de información, para brindar seguridad de la continuidad del servicio y protección de la información sensible, además de contar con muy poco apoyo para las unidades de tecnologías de información, por lo que CGR solicita a la Institución la implantación de las Normas Técnicas para la gestión y el control de las Tecnologías de Información actualmente vigente, aprobar y comunicar el Plan de Contingencias de TI; establecer un procedimiento para definir un portafolio de proyectos de infraestructura para el período 2013-2021

Además de que la Comisión de Gestión Informática, nombrada mediante resolución de la rectoría N.° R-048-2013 del 30 de enero de 2013, en su acta numero 1 había acordado utilizar **Objetivos de Control para Información y Tecnologías Relacionadas** (COBIT) para hacerle frente a los requerimientos y normas de la contraloría, pero además como herramienta estratégica para la utilización de buenas prácticas.

Por tal motivo la normativa a utilizar en este auditoria serán las siguientes:

- Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), emitida por la CGR, del 7 de junio, 2007. Publicada en La Gaceta Nro.119 del 21 de junio, 2007
- COBIT 5.
- Normas de Técnicas TI de la Institución.

1.4. Estudio preliminar

Cuando se realiza la visita preliminar para conocer el contexto donde se desarrolla el proyecto se encuentra que el personal y estudiantes indican que:

- se presenta fallas en las redes cableadas,

- que el cable se encuentra expuesto a la intemperie y pueden ser comidos por roedores, o pueden ser cortados por los funcionarios de mantenimiento por accidente
- o bien que pueden conectarse equipos especiales a ellos para el hurto de información,
- propiamente en el área donde realizan las labores el encargo de TI, se aprecian que las paredes que están hechas en madera está siendo comida por polilla y por comején, afectando la estructura física del cuarto principal.

Se logra observar que hay funcionarios que comparten las contraseñas de los usuarios con otros compañeros, que algunos de ellos no cambian la contraseña que se le asigna temporalmente y que el sistema no los obliga, etc.

Se nos indica que algunos de los equipos de la red interna ubicados para dar soporte a sectores de laboratorio fueron removidos del lugar y ahora lo están usando para impartir lecciones sin aprobación alguna del departamento de TI.

El acceso a los servidores no cuenta con ningún tipo de seguridad, no se cuenta con sistemas de respaldo eléctrico secundario, no hay equipo de monitorización.

Ante eventos que son potenciales hallazgos se hace necesario crear un programa de trabajo que verifique todo lo inicialmente observado, determinar si es permanente o fue circunstancial. Este estudio preliminar amplio el conocimiento para definir claramente los objetivos y alcance tanto del proyecto como de la auditoría a ejecutar.

CAPITULO II
DESARROLLO DEL TEMA

DESARROLLO DEL TEMA DE INVESTIGACIÓN

3.1 Actividades del Proyecto

Tal como se planteó en la metodología, la investigación abarca tres grandes macro-etapas: Planificación, Ejecución y Comunicación de resultados.

A continuación, se describe cada una de ellas:

3.1.1 Planificación

Esta etapa inicia con la tarea de identificar si los procesos actuales cumplen con la normativa e identificar la magnitud del impacto operacional y financiero de la entidad, si se interrumpe algunos de estos procesos.

Producto de la anterior indagación se determina la oportunidad y posibilidad real de llevar a cabo el trabajo con el alcance y en el tiempo establecido, así como los recursos requeridos.

Una vez determinada la viabilidad de cumplir con los objetivos del proyecto y de la empresa, se prepara el programa de ejecución del trabajo, para que una vez aprobado se comience a determinar las funciones y procesos importantes para la supervivencia de la empresa al momento de materialización de un riesgo que afecte la gestión de las TI de la sede, diseñar las herramientas para poder atender de extremo a extremo todo el programa de trabajo, diseñar los cuestionarios, las guías de entrevista y todas las plantillas de trabajo para evidenciar la ejecución del mismo.

3.1.1.1 Programa del Proyecto

En esta sección se detalla el proyecto a ejecutar en la institución pública de educación superior para evaluar la seguridad de la gestión en la sede del Pacífico.

Proyecto a ejecutar	**Evaluación de la seguridad de las Tecnologías de Información en un Centro Universitario del Pacífico**		
Responsable:	Javier Hernández González		
Aprobado por			
	Magister Wendy Vargas Hernández	**Firma**	**Fecha**
	Magister Ana P. Porras Solano	**Firma**	**Fecha**
Plazo de ejecución	De enero a marzo de 2018		

1. Objetivos del trabajo

Determinar la aplicabilidad de la normativa de TI en uno de los centros desconcentrados de soporte informático de la universidad, a través de un análisis del cumplimiento de la normativa institucional en materia de Tecnologías aprobada por la Comisión institucional de Gestión Informática en 2016.

2. Naturaleza

El presente trabajo se realiza como proyecto de graduación para obtener el grado de Magister en Auditoría de Tecnologías de Información del Programa de Posgrado en Administración y dirección de Empresas de la Universidad de Costa Rica.

3. Alcance

Se basará en el cumplimiento de las políticas y otra normativa propia para la administración de las tecnologías en lo que corresponde a la Evaluación de la seguridad de las Tecnologías de Información en un Centro Universitario del Pacífico, oficializadas por la Comisión institucional de Gestión Informática y su aplicación en la sede del pacífico (Puntarenas), evaluando lo actuado en esta sede hasta diciembre 2017.

4. Procedimientos de trabajo

Procedimientos a Evaluar			
ID	**Detalle**	**Ref. PT**	**Tiempo estimado**
1	1.4.1 DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información • Control de software instalado • Control de incidencias de contraseñas • Control de usuarios inactivos • Control de correo electrónico Anti-Spam • Percepción de las políticas y procedimientos de seguridad de la información • Control del Ambiente Físico • Control de ejecución de pruebas de continuidad • Mantenimiento del Esquema de Clasificación de Datos • Actualización de documentación		10 días
2	1.4.1 DGTI-EA-0116 Esquema de Clasificación de la Información • Disposiciones Generales sobre Activos de Información • Disposiciones Generales de Seguridad • Clasificación de la Información		5 días
3	1.4.3 DGTI-PA-17 Política Seguridad Física y Ambiental • Acceso y monitoreo del ambiente físico • Incidentes de seguridad		3 días

4	1.4.3 DGTI-PO-3300020 Procedimiento Acceso a Instalaciones Restringidas de TI • Control de Visitantes a Instalaciones Restringidas de TI	2 días
5	1.4.3 DGTI-PO-3300030 Procedimiento Monitoreo del Ambiente Físico • Monitoreo de instalaciones restringidas de TI • Revisión de accesos • Revisión de monitoreo y mantenimientos	2 días
6	1.4.3 DGTI-PO-5305010 Procedimiento Desecho y Reutilización de Equipo de TI • Reutilización del Equipo de TI • Desecho del Equipo de TI	2dias
7	1.4.4 DGTI-PO-3300040 Procedimiento Gestión de Incidentes de Seguridad • Detección de Incidentes de Seguridad • Valoración de Incidentes de Seguridad • Atención de Incidentes de Seguridad • Seguimiento y Cierre de Incidentes de Seguridad • Evaluación de Incidentes de Seguridad	5 días
8	1.4.4 DGTI-PO-5100020 Procedimiento Protección contra Software Malicioso • Prevención y Detección de Software Malicioso	2 días
9	1.4.4 DGTI-PO-5107010 Procedimiento Gestión de Respaldos y Restauraciones • Solicitud de Respaldo • Solicitud de Restauración • Pruebas de Respaldos y Restauraciones	3 días
10	1.4.4 DGTI-PO-5406010 Procedimiento Tratamiento de Medios de Almacenamiento • Eliminación de Datos • Destrucción de Medios de Almacenamiento	3 días
11	1.4.5 DGTI-PO-3300050 Procedimiento Control de Acceso	10 días

- Creación de Cuentas de Dominio/Sistemas
- Modificación de Cuentas
- Deshabilitar, Habilitar o Eliminar Cuentas
- Restablecer Contraseñas o Desbloquear Cuentas
- Monitoreo de Cuentas y Accesos

CAPITULO III
ETAPA DE COMUNICACIÓN

INFORME DE EVALUACIÓN DE LA NORMA DE TI APLICADA EN SEDE PACIFICO

1. Aspectos generales

1.1. Origen de la Evaluación

Durante los últimos años se han identificado múltiples debilidades en la gestión de la seguridad de las TI en la Sede Pacífico, situación que ha sido advertida en distintos informes dirigidos a la Dirección de la Sede por diferentes actores; situación que pone en riesgo la información institucional, la calidad y continuidad de los servicios y el debido cumplimiento del marco normativo aplicable a la organización"; razón por la cual resulta imperante evaluar tal condición a fin de identificar las acciones de mejora que se deben atender oportunamente para mitigar tales riesgos y promover el logro de los objetivos institucionales soportados con los recursos de TI."

1.2. Objetivo de la Evaluación

Verificar la razonabilidad de cómo se están aplicando y se mantienen los controles definidos en la normativa institucional y cómo aseguran la integridad de la información, la satisfacción del negocio y la continuidad de las operaciones de los servicios que presta la institución en la sede del Pacífico. Concordante con la tesis

1.3. Alcance de la evaluación

La auditoría comprenderá la evaluación de la razonabilidad y eficacia de los controles internos establecidos institucionalmente en la Sede Pacifico para el debido cumplimiento de las normas aplicables a la gestión de TI, durante el periodo 2017.

1.4. Antecedentes de la Entidad

La Universidad Técnica Nacional nació como resultado de la fusión legal de las siguientes instituciones de educación técnica superior (Universidad Técnica Nacional, 2015): CUNA, CUP, CURDTS, ECAG, CIPET, CEFOF, contando con una larga experiencia académica y una valiosa trayectoria histórica, la cual permitió el proceso de integración académica inicial de la Universidad, alcanzando muy rápidamente una amplia y diversificada oferta educativa.

La Universidad Técnica Nacional Sede del Pacífico está ubicada en la provincia de Puntarenas, Recinto Tobías Vargas en Puntarenas Centro: 100 metros al oeste del Muelle de Cruceros sobre el Paseo de los Turistas, frente a la Concha Acústica, en el edificio de la antigua aduana. (Universidad Técnica Nacional, 2015). Cuenta con un edificio de 10.000 m2 donde se llevan a cabo las funciones administrativas y docentes (Universidad Técnica Nacional, 2015), y con el Recinto Campus Juan Rafael Mora Porras, inaugurado en enero del año 2011, ubicado en El Roble de Puntarenas; antigua finca Socorrito, Costado sur del plantel de CoopeRoble R.L.

2. Hallazgos de Auditoría

2.1. Debilidades relacionadas con el procedimiento de control y seguimiento de seguridad de la Información, subproceso Control de software instalado.

Condición

- No se encontró evidencia de que el personal de seguridad de la Institución realizara muestras para la ejecución de la revisión de Software, a pesar de que en la DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información, establece que para prevenir riesgos de integridad y confiabilidad de los datos se debe determinar una muestra donde se

prueben la suficiencia de los controles establecidos para mitigar dichos riesgos.

- Como el software requiere equipos para ejecutarse, la normativa también deja claramente establecido que el personal de Seguridad de la Información, tiene entre sus responsabilidades verificar cómo están instalados y configurados los equipos donde se instalará el software de acuerdo con el Manual de Estándares de Equipo de TI, sin embargo, se evidenció que este personal de seguridad no se apersona a la sede a realizar esta labor.

  Lo que se encontró es que en Sede quien se encarga de la instalación de los equipos administrativos es el Coordinador de Sede, que no si bien es ingeniero de sistemas no es parte del personal de seguridad al que la normativa le asigna esta responsabilidad, aunado a que su labor no es verificada por seguridad institucional, ni se emite el Informe Técnico que le correspondería realizar al personal de seguridad una vez evaluada la compatibilidad de equipos y en consecuencia tampoco se ubicaron informes remitidos a la Dirección de la DGTI como establece la normativa, solamente , el emiten informes técnicos en caso que el activo que se está adquiriendo trae algún tipo de defecto o bien si no es lo que se ha solicitado por la dependencia, pero lo hace el Coordinador de sede cuando recibe el activo no como parte de un control de seguridad.

- Los roles de los accesos son controlados mediante un servidor en WINDOWS SERVER el cual posee configurado un Active Directory, la estación local posee un usuario administrador, con clave que solo la posee el coordinador, pero lo que corresponde a laboratorios poseen encargados de laboratorios los cuales son los que se encargan del mantenimiento del equipo, y solo se hace cargo del mantenimiento del equipo el coordinador, solo si el personal no sabe cómo

solucionar el problema, sin embargo esta situación no es controlada por el personal de seguridad que debe verificar el uso de software no autorizado.

- Se determinó que el personal de seguridad de la información no maneja un adecuado control de los activos, cuando se realiza la solicitud de equipos nuevos, el coordinador guía al personal de las distintas dependencias para elegir el equipo necesario basado en el Manual de Estándares de Equipó de TI, dichos equipos son ubicados en las dependencias según indique activos fijos en concordancia con lo que cada área o dependencia eligió mediante órdenes de compra.

Criterio

La condición descrita incumple la Normativa de TI 1.4. Gestión de la Seguridad de la Información, Implementación de un Marco de Seguridad de la Información DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información, en su subproceso Control de software instalado reza lo siguiente:

- El personal de la Seguridad de la Información debe determinar cuál será la población meta que funcionará como muestra para la ejecución de la revisión, con el fin de determinar los posibles riesgos a la integridad y confidencialidad de los datos debido al uso de software no permitido.
- El personal de Seguridad de la Información verificará que el equipo instalado en las locaciones evaluadas está acorde con lo establecido en el Manual de Estándares de Equipo de TI.
- Una vez evaluada la compatibilidad de los equipos, el personal de Seguridad de la Información deberá generar un informe técnico con los hallazgos encontrados.
- El personal de Seguridad de la Información presenta el informe a la Dirección de la DGTI.

Causa

La causa determinada es que Institución no cuenta con personal en el área de seguridad aun, por lo que los procedimientos anteriores no son llevados a cabo por dicho personal, sino más bien por el Coordinador de TI de la sede, a pesar de que no es el especializado en materia de seguridad de la información.

Efecto

El incumplimiento a la DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información genera que los riesgos que se pretendieron mitigar con su definición, no se tiene una seguridad razonable de que el software y hardware asociado a la gestión estén preparados adecuadamente ante una contingencia. Otro efecto de este descontrol de activos es la ausencia de un inventario de equipos y licencias adquiridas, así también como un registro de instalaciones (equipos con licencias permitidas), de modo que se determine la suficiente autorización para cubrir todos los equipos y los programas en uso y cumplir con la protección de los derechos de autor relativos en lo que a programas de cómputo se refiere.

Recomendación1: Al Director de TI

Se recomienda, tomar las acciones necesarias para asegurar de manera razonable el control del software instalado, así como la adquisición de hardware y software para los recintos como la sede del Pacífico y cualquiera otra que se encuentre en estas condiciones, de forma que se mitiguen adecuadamente los riesgos asociados a este subproceso, en cual debe contemplar, entre otras cosas, pero no únicamente:

a. Ejecutar revisiones periódicas que determinen los posibles riesgos a la integridad y confidencialidad de los datos debido al uso de software no permitido.

b. Verificar que el equipo instalado (actualmente y que se adquiera) en las locaciones evaluadas esté acorde con lo establecido en el Manual de Estándares de Equipo de TI.

Recomendación2: Al Director de TI

Presupuestar y ejecutar lo necesario para contar, a corto plazo, con el personal de Seguridad de la Información que debe cumplir con la Normativa de TI 1.4. Gestión de la Seguridad de la Información:

a. A corto plazo. Capacitando el personal actual

b. Largo plazo. Solicitar presupuesto y plazas para contratar al personal de seguridad de Información específico.

Recomendación 3: Al Director de TI

Se recomienda mantener actualizado el inventario de la infraestructura tecnológica institucional y local en cada sede, de forma que se controle integral y locamente los activos asociados a la Seguridad de la información, tanto a nivel de redes, hardware como de licenciamiento.

2.2. Debilidades relacionadas con el procedimiento control y seguimiento de seguridad de la Información subproceso Control de incidencias de contraseñas:

Condición

Ante la ausencia de un procedimiento institucional estándar y la definición de un responsable específico, en la Sede Pacífico la creación de los usuarios, se realiza mediante la solicitud del director o jefe del área, mediante correo, boleta o solicitud a la Mesa de trabajo soporte.pacifico@utn.ac.cr, así como también la solicitud la asignación nuevamente de una contraseña temporal. El vencimiento

de la contraseña está regido por las políticas de contraseñas establecidas en Windows server 2012 en el Active Directory y no por políticas institucionales.

Los datos son recolectados en las boletas, y en la mesa de trabajo, sin embargo, algunos usuarios optan por realizarla mediante correo electrónico al Coordinador de Sede en cuyo caso este se encarga de redirigirlo a la mesa de trabajo.

El Active Directory de Windows controla los tiempos de vigencia de la contraseña de los usuarios según se configuro por el administrador o el coordinador de sede en su momento.

Ante lo anterior la sede administra los accesos y no se extrae la información sobre incidentes al vencimiento de contraseña o incumplimientos a las políticas de cambio de contraseñas, en consecuencia, no se identifican las causas raíz de los incidentes, sino que se atienden cuando se presentan y a veces reinciden.

Según la normativa de TI La Normativa de TI 1.4. Gestión de la Seguridad de la Información, Implementación de un Marco de Seguridad de la Información DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información, en su subproceso Control de incidencias de contraseñas reza lo siguiente:

- Extraer información sobre incidentes presentados por el vencimiento de contraseñas, identificando el cumplimiento de las políticas de cambios de contraseña.
- Recolección de datos sobre incidentes asociados al uso de contraseñas.
- Identificar la causa raíz de los incidentes relacionados con el vencimiento de contraseñas. De identificarse, presentar un plan de acción para análisis a la Dirección de la DGTI.

De forma que se logren identificar los motivos por los cuales se solicita los cambios de contraseñas, además de la creación de planes de acción para minimizar dichas incidencias.

Causa

La causa de la situación en comentario, es que no se define en el procedimiento persona responsable de realizar las tareas indicadas en el procedimiento ni se monitorea por parte de la DGTI pues no se evidenció revisión de lo que realiza la sede del Pacífico.

Efecto

El no definir el responsable de las tareas en el procedimiento indicado, impide a la Dirección de TI establecer compromisos y obligaciones del personal sobre dichos procesos, lo cual provoca incertidumbre sobre quien o quienes deben llevar a cargo el proceso.

Incumple también con la ley protección de los derechos de autor, pues el control de accesos es vital para identificar los responsables y otros elementos de seguridad que se filtran en la red institucional.

Recomendación 4: Al Director de TI.

Se recomienda definir la responsabilidad sobre el proceso Control de incidencias de contraseñas, definiendo el puesto que se encargará de este proceso y las funciones específicas que debe llevar a cabo.

Recomendación 5: Al Director de TI.

Dar a conocer a nivel institucional las políticas establecidas sobre las contraseñas, su aplicación y sanciones por el incumplimiento. Además de definir un sitio común en la intranet para que estén disponibles para todos los usuarios.

2.3. Debilidades relacionadas con el procedimiento control y seguimiento de seguridad de la Información subproceso Control de usuarios inactivos.

Condición

Se identifica que en la Sede Pacífico el Departamento de Gestión de Desarrollo Humano se encarga de enviar correos solicitando la desactivación delas cuentas de correos del personal que ha finalizado en forma temporal o permanente su relación contractual con la Universidad al Coordinador de Sede o bien a la mesa de trabajo soporte.pacifico@utn.ac.cr, mientras que el jefe del departamento, el director de área, o el decano(a) es el que se encarga de solicitar la desactivación de los cuentas de usuarios de los equipos y de cualquier otro acceso a los sistemas que poseen.

El Coordinador de Sede, se encarga de proceder en desactivar el correo de la persona, y accesos a sistemas de sede, y el usuario del Active Directory según se tramito, sin embargo, no se ha establecido limitaciones de tiempo de acceso a los usuarios ya que el personal en ocasiones cumple horarios hasta tarde por diferentes motivos, y requieren del acceso para cumplir con los trabajos; el cambio de los accesos de los usuarios solo se realiza cuando se envía una solicitud.

Se observó que el Coordinador de Sede realiza charlas al personal para concientizar la importancia de no compartir contraseñas de los equipos, del correo y de los sistemas, pero no se basa en un procedimiento formalmente establecido para control de accesos.

Criterio

Según la normativa de TI La Normativa de TI 1.4. Gestión de la Seguridad de la Información, Implementación de un Marco de Seguridad de la Información DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información, en su subproceso Control de usuarios inactivos, la institución establece procedimientos para la desactivación de cuentas de personal que han finalizado en forma temporal o permanente su relación contractual con la Universidad a cargo del personal de seguridad de TI.

Causa

La causa de la situación en comentario, es la ausencia de personal de seguridad institucional específicos que verifiquen el cumplimiento y la razonabilidad de lo que define cada sede respecto a horarios y controles de acceso.

Efecto

Se incrementa la probabilidad de un acceso no autorizado, dado que si un jefe no solicita el cambio en el acceso sea horarios o tiempo de vigencia, o si recursos humanos olvida comunicar el cese de labores, pueden tener acceso personas que pueden permitir malware o robo de información confidencial.

Recomendación 6: Al Director de TI

Se recomienda realizar una evaluación de los perfiles de los usuarios que tienen asignada una contraseña y determinar, según la necesidad de uso, los horarios y acceso que deben tener vigentes a cada perfil

Establecer normativa que oficialice y dé a conocer estas condiciones tanto a los usuarios a los que se les aplicará como al profesional técnico que se le asignará la responsabilidad de ejecutar este control.

Recomendación 7: Al Director de TI

Dar a conocer el procedimiento DI-PRO-04 Procedimiento de Soporte y cualquiera otro asociado con el control de usuarios y ponerlo a disponibilidad en la Intranet.

2.4. Debilidades relacionadas con el procedimiento control y seguimiento de seguridad de la Información subproceso Percepción de las políticas y procedimientos de seguridad de la información.

Condición

Se identifica que en la Sede Pacífico no se realizan muestreos para determinar si el personal posee conocimientos sobre seguridad de la información a pesar de que así lo establece la Normativa de TI 1.4. Gestión de la Seguridad de la Información, Implementación de un Marco de Seguridad de la Información DGTI-PO-3300010 Percepción de las políticas y procedimientos de seguridad de la información.

Criterio

Según la normativa de TI La Normativa de TI 1.4. Gestión de la Seguridad de la Información, Implementación de un Marco de Seguridad de la Información DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información, en su subproceso Percepción de las políticas y procedimientos de seguridad de la información, la institución establece procedimientos para determinar el conocimiento del personal sobre la seguridad de información.

Causa

La causa de la situación en comentario, es la falta de personal de seguridad que ejecute los procedimientos que se detallan.

Efecto

La situación en comentario incrementa el riesgo de incumplimientos por parte de los usuarios sobre todo de nuevo ingreso de las medidas de seguridad que deben cumplir y de tampoco se pueden sentar responsabilidades al no poder identificar los causantes.

Recomendación 8: Al Director de TI

Identificar las causas que le impiden cumplir con lo establecido en Normativa de TI 1.4. Gestión de la Seguridad de la Información, y tomar las medidas que aseguren que a corto plazo se pueda ejecutar a cabalidad esta normativa.

2.5. Debilidades relacionadas con el procedimiento control y seguimiento de seguridad de la Información subproceso Control del Ambiente Físico.

Condición

Se identifica que en la Sede Pacífico no se realiza solicitado por parte del personal de seguridad de la información sobre los ambientes físicos, ni se realiza revisiones mensuales. En caso de presentarse hallazgos el coordinador de TI genera informes técnicos para indicar sobre las situaciones presentadas pero las acciones correctivas no siempre se ejecutan con la prontitud requerida y algunos aspectos físicos presentan deterioro.

Criterio

Según la normativa de TI La Normativa de TI 1.4. Gestión de la Seguridad de la Información, Implementación de un Marco de Seguridad de la Información DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la

Información, en su subproceso Control del Ambiente Físico, la institución establece procedimientos para determinar que no existan desviaciones sobre los ambientes físicos de TI.

Causa

La causa de la situación en comentario, es la ausencia de personal de seguridad que ejecute los procedimientos que se detallan aunado a que el coordinador de esta área, aunque se esfuerce por mantener el ambiente adecuado los recursos no siempre los tiene a disposición.

Efecto

La situación en comentario ha generado deterioro de los ambientes físicos de TI y el incumplimiento con el Marco de Seguridad de la Información DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información, en su subproceso Control del Ambiente Físico.

Recomendación 9: Al director de TI

Identificar las causas que le impiden cumplir con lo establecido el Marco de Seguridad de la Información DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información, en su subproceso Control del Ambiente Físico, y tomar las medidas que aseguren que a corto plazo se pueda ejecutar a cabalidad esta normativa y buscar acciones correctivas.

3. Conclusión del Informe

En la evaluación se valoró la efectividad y correcto funcionamiento de los controles de la normativa; si dichos procesos son válidos, completos, precisos, oportunos y seguros; la suficiencia de los controles para la gestión de las normativas; si se aplican controles para un aseguramiento de los datos, de los activos y finalmente, si se aplican controles de índole técnica y de organización para asegurar la seguridad de los datos institucionales.

Se determinaron una serie de aspectos sujetos a mejora que pueden brindar un valor agregado no solo a la seguridad de la información de la sede del Pacífico, sin que permitirá a la UTN, verificar en temas puntuales si estas condiciones se repiten en otras sedes del territorio nacional y atacar un potencial problema institucional.

Por otro lado, se identificó una causa común en más del 80% de las condiciones señaladas: la ausencia del personal de seguridad que exige la normativa indicada, normativa que fue aprobada y puesta en vigencia sin contar con todos los elementos necesarios para que la pudiese ejecutar los responsables asignados a su cumplimiento, lo que deja en evidencia un deficiente o nulo estudio de factibilidad.

Las deficiencias de control de aplicación de la normativa por falta de personal de seguridad que la aplique; y debilidades relacionadas con la aplicación de controles para proteger los medios de comunicación y los hallazgos señalados, deja en evidencia la urgencia de proveer a la sede del Pacífico de UTN los recursos necesarios para llevar a cabalidad el cumplimiento de la normativa.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Implementar políticas de seguridad en la Universidad Técnica Nacional permite proteger, preservar, administrar eficientemente los recursos con que se cuenta, además de su aplicación permite prevenir, evitar, controlar y minimizar las averías de incidentes que la afectan o que podrían afectar a la institución, además de que aplicar evaluaciones periódicas a dichas normativas permite corroborar situaciones que no cubren la normativa, o si lo implementado se está aplicando correctamente.

Surge la necesidad en Sede capacitar al personal para que éste pueda tomar un papel activo dentro de la organización de manera que aplique los protocolos, controles, procedimientos, directrices, manuales, reglamentos dispuestas en la Normativa de TI, con el propósito de proteger de una forma adecuada la información, y activos que se le confía. De esta forma contar con el apoyo y participación de todas las Direcciones, áreas, Departamentos y lograr así cumplir los objetivos planteados a lo interno de la institución.

Por tratarse el trabajo a la evaluación de la normativa y su aplicación en sede pacifico, el ámbito de aplicación de la normativa de TI de UTN no se aplica en forma general ya que hay procedimientos y controles que no aplican a Sedes.

Además, con la aplicación de la presente evaluación se logra determinar oportunidades de mejora para el fortalecimiento a la normativa, como son los casos de la protección de la red LAN en las Sede Pacifico, las protecciones de descargas atmosféricas o de seguridad a causa de fenómenos naturales, y muchas otras que no son tomados en la normativa actual.

Recomendaciones.

- Contar con ciclo de mejora continua de la normativa en la que aplique programas de difusión, monitoreo, revisión y actualización

- Desarrollar políticas para capacitar al personal en lo que a la normativa se refiere ya que no existe aún ninguna.

- Tomar en cuenta cuando implementen normativas a las áreas involucradas de forma tal que las políticas de áreas, direcciones, etc. no se contradigan una con otra.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

ASAMBLEA LEGISLATIVA. (2008). *LEY ORGÁNICA DE LA UNIVERSIDAD TÉCNICA NACIONAL*. San Jose, Costa Rica.: La Gaceta.

Asamblea Legislativa de la República de Costa Rica. (2008). LEYES 8638 Ley Orgánica de la Universidad Técnica Nacional. 10. Obtenido de LEYES 8638 LEY ORGÁNICA DE LA UNIVERSIDAD TÉCNICA NACIONAL.

Barrantes Echavarría, R. (1999). *Investigación: Un camino al conocimiento, Un enfoque cuantitativo y cualitativo.* (1era ed., Vol. 1era Edición). San José, San José, Costa Rica: Universidad Estatal a Distancia. Recuperado el 28 de 9 de 1997

Contraloría General de la República. (21 de Junio de 2007). Normas técnicas para la gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE). San José, San José, Costa Rica: La Gaceta .

Contraloría General de la República. (2013). *INFORME N° DFOE-SOC-IF-12-2013 INFORME SOBRE EL PROCESO DE CONFORMACIÓN Y CONSOLIDACIÓN DE LA UNIVERSIDAD TÉCNICA NACIONAL*. San josé: Contraloría General de la República.

Contraloría General de la República. (2013). *INFORME NO. DFOE-SOC-IF-04-2013 INFORME SOBRE LA ORGANIZACIÓN Y FUNCIONAMIENTO DE LA DIRECCIÓN DE AUDITORÍA INTERNA DE LA UNIVERSIDAD TÉCNICA NACIONAL*. San José: Contraloría General de la República.

Contraloría General de la República. (25 de Setiembre de 2014). Normas Generales de Auditoría para el Sector Publico. *Normas Generales de Auditoría para el Sector Publico*. San José, San José, Costa Rica: La Gaceta.

Universidad Técnica Nacional . (2015). *Reseña Histórica de la Universidad Técnica Nacional*. Obtenido de Reseña Histórica de la Universidad Técnica Nacional: http://www.utn.ac.cr/content/rese%C3%B1a-hist%C3%B3rica-de-la-universidad-t%C3%A9cnica-nacional

Universidad Técnica Nacional . (1 de Setiembre de 2016). Modelo Educativo Una universidad innovadora para la Costa Rica del siglo XXI. Alajuela, Alajuela, Costa Rica. Obtenido de Modelo Educativo: http://www.utn.ac.cr/content/modelo-educativo

UNIVERSIDAD TÉCNICA NACIONAL. (2010). R-048-2013 SE REORGANIZA LA COMISION INSTITUCIONAL DE GESTION. ALAJUELA, ALAJUELA, Costa Rica.

Universidad Técnica Nacional. (2013). ACTA No. 15 CONSEJO UNIVERSITARIO DE LA UNIVERSIDAD TÉCNICA NACIONAL SESIÓN ORDINARIA No.46-2013. Alajuela, Alajuela, Costa Rica.

Universidad Técnica Nacional. (2015). *Descripción de la Sede*. Obtenido de Descripción de la Sede: http://www.utn.ac.cr/sedes/sede-regional-de-pac%C3%ADfico

Universidad Técnica Nacional. (2015). *Marco Estratégico*. Obtenido de http://www.utn.ac.cr/content/marco-estrat%C3%A9gico

Universidad Técnica Nacional. (2015). *Sede Regional de Pacífico*. Obtenido de http://www.utn.ac.cr/sedes/sede-regional-de-pac%C3%ADfico?type=3

Universidad Técnica Nacional. (2015). *Ubicación de nuestras Sedes*. Obtenido de Ubicación de nuestras Sedes: http://www.utn.ac.cr/mapas-y-direcciones

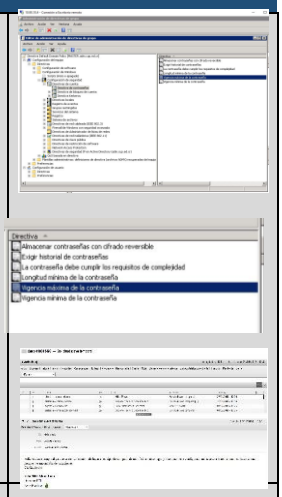
Universidad Técnica Nacional. (2016). *Plan Estratégico de Tecnologías de Información y Comunicación (PETIC).* Alajuela: UTN.

ANEXOS

Etapa de Examen

EVALUACIÓN DE NORMATIVA 1.4. Gestión de la Seguridad de la Información Aplicada en UTN Sede Pacífico: 1.4.1. Implementación de un Marco de Seguridad de la Información	REF:	HT-01
	Hecho por:	JAHG
	Fecha:	1-May-18
	Revisado por:	
	Fecha:	

ÍTEM	PREGUNTA	Aplicación	JUSTIFICACIÓN	EVIDENCIAS
1.4.1.1. DGTI-PO-3300010 Procedimiento Control y Seguimiento de Seguridad de la Información				
1.4.1.1.1. Control de software instalado				
.1	El personal de la Seguridad de la Información debe determinar cuál será la población meta que funcionará como muestra para la ejecución de la revisión, con el fin de determinar los posibles riesgos a la integridad y confidencialidad de los datos debido al uso de software no permitido.	NO APLICA	En Sede Pacífico todo el equipo Administrativo es instalado, revisado, reparado, por el Coordinador de Sede, todo el software que se instala según las licencias con las que cuenta la Universidad, y la única persona que posee el roll de Administrador es en el encargado de la Coordinación, el resto de los empleados poseen roll de usuario, esto esta contralado por un Windows Server con Active Directory.	
.2	¿Es de su conocimiento el Manual de Estándares de Equipo de TI?	SÍ	El coordinador de Sede guía a las diferentes dependencias en las adquisiciones de equipos, en los periodos de tiempos establecidos.	
.3	El personal de Seguridad de la Información verificará que el equipo instalado en las locaciones evaluadas está acorde con lo establecido en el Manual de Estándares de Equipo de TI.	NO APLICA	En sede Pacífico equipo es asignado según como es enviado desde Alajuela y según indica activos fijos	
.4	Una vez evaluada la compatibilidad de los equipos, el personal de Seguridad de la Información deberá generar un informe técnico con los hallazgos encontrados.	NO APLICA		
.5	El personal de Seguridad de la Información presenta el informe a la Dirección de la DGTI.	NO APLICA	El coordinador de sede emite informes Técnicos solo si los equipos presenta problemas, o no es lo solicitado.	

1.4.1.1.2. Control de incidencias de contraseñas:				
.1	Extraer información sobre incidentes presentados por el vencimiento de contraseñas, identificando el cumplimiento de las políticas de cambios de contraseña.	NO APLICA	En la Sede Pacífico la asignación de la contraseña de los usuarios, se realiza mediante la solicitud del director o jefe del área mediante correo, boleta o solicitud a la Mesa de trabajo soporte.pacifico@utn.ac.cr, así como también la solicitud nuevamente de la contraseña por cualquier motivo que sea, el vencimiento de la contraseña está regido por las políticas de contraseñas establecidas en el Active Directory.	
.2	Recolección de datos sobre incidentes asociados al uso de contraseñas.	NO APLICA	Los datos son recolectados en las boletas, y en la mesa de trabajo, si se realiza mediante correo electrónico al Coordinador de Sede este se encarga de redirigirlo a la mesa de trabajo.	
.3	Identificar la causa raíz de los incidentes relacionados con el vencimiento de contraseñas. De identificarse, presentar un plan de acción para análisis a la Dirección de la DGTI.	NO APLICA	El active directory de Windows controla los tiempos de vigencia de la contraseña de los usuarios según se configuro por el administrador o el coordinador de sede en su momento	
1.4.1.1.3. Control de usuarios inactivos				
.1	Se solicita a la Dirección de Recursos Humanos un listado de las personas que han finalizado en forma temporal o permanente su relación contractual con la Universidad en los últimos seis meses, por parte del personal de Seguridad de la Información.	NO APLICA	En la Sede Pacífico el Departamento de Gestión de Desarrollo Humano se encarga de enviar correos solicitando la desactivación de los de usuarios que han finalizado en forma temporal o permanente su relación contractual con la Universidad al Coordinador de Sede o bien a la mesa de trabajo soporte.pacifico@utn.ac.cr	
.2	El personal de la Seguridad de la Información debe hacer una referencia cruzada entre la lista proporcionada por la Dirección de Recursos Humanos con el listado de usuarios de aplicaciones y del dominio de la Institución en los últimos seis meses.	NO APLICA	Coordinador de Sede, se encarga de proceder en desactivar el correo de la persona, y accesos a sistemas de sede, y el usuario del Active Directory.	
.3	Se han Desactivados usuarios que están fuera por periodos de tiempo prolongados.	NO	En la Sede ningún jefe o Director ha Solicitado la desactivación del usuarios de personal que está afuera de	

			la institución por periodos prolongados	
.4	Se ha Monitoreado el acceso de usuarios a equipos y sistemas, identificando si una cuenta ha sido accedida en tiempos inusuales. Para lo cual, se pueden dar diferentes escenarios.	**NO**	No se ha establecido limitaciones de tiempo de acceso a los usuarios ya que el personal en ocasiones cumplen horarios hasta tarde, y requieren del acceso para cumplir con los trabajos.	
.5	Se desactivan derechos al cambiar personal de departamentos	**NO APLICA**	la desactivación de los derechos de los usuarios solo se desactivan, cuando es solicitado por el director o jefe del departamento	
.6	¿Se realiza conciencia al personal de no compartir las contraseñas?	**SÍ**	El Coordinador de Sede les habla al personal la importancia de no compartir las contraseñas, y en años anteriores se han realizado charlas para al personal	
.7	Es de conocimiento del coordinador de Sede el Procedimiento DI-PRO-04	**NO**		
.8	El personal de Seguridad de la Información reporta a la DGTI los hallazgos identificados, para que se analice el informe y se tomen las medidas necesarias en caso de existir incumplimientos a los lineamientos de seguridad de la información.	**NO APLICA**		
1.4.1.1.4. Control de correo electrónico Anti-Spam				
.1	Seguridad de la Información solicita las medidas anti-spam existentes en el correo institucional al área de Gestión Técnica, quienes envían el listado respectivo.	**NO APLICA**		
.2	El personal de Seguridad de la Información evalúa las medidas anti-spam para el bloqueo de sitios o dominios de correo no seguros o de dudosa procedencia.	**NO APLICA**		
.3	El personal de la Seguridad de la Información estudia los casos e incidentes reportados por los usuarios, considerando la actualización de las políticas del servidor de correo.	**NO APLICA**		
.4	El personal de Seguridad de la Información genera acciones correctivas para mitigar el riesgo de un ataque por medio de correo electrónico.	**NO APLICA**		
.5	El personal de Seguridad de la Información capacita a los usuarios sobre las amenazas de	**NO APLICA**		

	correo electrónico, indicando la forma de reportarlos a la Dirección de Gestión de Tecnologías de la Información.			
1.4.1.1.5. Percepción de las políticas y procedimientos de seguridad de la información				
.1	El personal de Seguridad de la Información define la población meta que servirá como muestra para la ejecución de encuestas, que permitan la evaluación del conocimiento general sobre seguridad de la información en la institución.	**NO APLICA**		
.2	Definir estructura y contenido de las encuestas a realizar.	**NO APLICA**		
.3	Aplicar las encuestas al personal designado como población meta.	**NO APLICA**		
.4	Tabular las respuestas a las encuestas y generar un consolidado de la información.	**NO APLICA**		
.5	Reportar para el respectivo análisis a la Dirección de la DGTI, los resultados obtenidos en las encuestas, con el objetivo de que tomen las medidas necesarias.	**NO APLICA**		
1.4.1.1.6. Control del Ambiente Físico				
.1	El personal de Seguridad de la Información solicita documentación existente sobre el ambiente físico a la jefatura correspondiente.	**NO APLICA**		
.2	Seguridad de la Información realizará revisiones mensuales sobre la normativa de infraestructura tecnológica, con el objetivo de evaluar el cumplimiento de los requerimientos de ambiente físico y la actualización de la documentación.	**NO APLICA**		
.3	En caso de identificar desviaciones, el personal de Seguridad de la Información deberá reportar los hallazgos identificados en la evaluación previa, a la Dirección de la DGTI.	**NO APLICA**		
.4	La Dirección de DGTI en conjunto con el personal de Seguridad de la Información deberá analizar las medidas de acción/prevención a tomar en cuenta, según los hallazgos identificados.	**NO APLICA**		
1.4.1.1.7. Control de ejecución de pruebas de continuidad				
.1	El personal responsable debe calendarizar y coordinar la ejecución de las pruebas de	**NO APLICA**		

	recuperación del plan de continuidad de TI, en períodos semestrales.			
.2	Determinar fecha y periodo de ejecución de las pruebas.	**NO APLICA**		
.3	Coordinar los recursos de equipo y personal necesarios para la ejecución de las pruebas.	**NO APLICA**		
.4	Llevar a cabo las pruebas que contempla el Plan de Continuidad, según el personal y recursos involucrados.	**NO APLICA**		
.5	Realizar un consolidado de los resultados, resaltando las oportunidades de mejora o deficiencias identificadas en el Plan de Continuidad.	**NO APLICA**		
.6	En caso de existir desviaciones, determinar las acciones para mitigar los problemas generados durante las pruebas.	**NO APLICA**		
.7	Reportar los hallazgos identificados, así como las medidas tomadas producto de las pruebas, a la Dirección de la DGTI y al personal responsable de Seguridad de la Información.	**NO APLICA**		
1.4.1.1.8. Mantenimiento del Esquema de Clasificación de Datos				
.1	El personal de Seguridad de la Información de la DGTI actualiza el Esquema de Clasificación de Datos, estableciendo los estratos y lineamientos generales de seguridad. Una vez finalizado, el personal de Seguridad de la Información remite a la Dirección de la DGTI el Esquema de Clasificación de Datos para su análisis.	**NO APLICA**		
.2	Cada área del DGTI establece los controles según los lineamientos generales establecidos en el Esquema de Clasificación de Datos, para los datos de su ámbito.	**NO APLICA**		
.3	Las áreas de TI documentan los lineamientos técnicos para cada estrato del Esquema de Clasificación de Datos, de acuerdo a su competencia técnica, y lo remiten al Comité de Seguridad.	**NO APLICA**		
.4	El Comité de Seguridad válida los lineamientos presentados por cada área de TI. De llegar a un consenso y ser aceptados, los lineamientos son aprobados. Caso contrario se solicitan los ajustes al	**NO APLICA**		

	área de TI correspondiente.			
.5	El personal de Seguridad de la Información realiza revisiones periódicas para valorar la aplicación de los lineamientos de seguridad.	**NO APLICA**		
1.4.1.1.9. Actualización de documentación				
.1	El personal de Seguridad de la Información actualiza anualmente los procedimientos y políticas relacionados con el marco de seguridad de la información, proceso que establece: · Revisión de documentación · Validación de cambios · Realización de cambios o actualizaciones · Envío de documentación a la Dirección	**NO APLICA**		
.2	Las actualizaciones serán revisadas y aprobadas por la Dirección del DGTI.	**NO APLICA**		
1.4.1.2. DGTI-EA-0116 Esquema de Clasificación de la Información				
.1	Conoce sobre la conformación del Comité de Arquitectura de Información	**NO APLICA**		
.2	Conoce sobre la conformación de la Comisión de Institucional de Gestión Informática (CIGI)	**NO APLICA**		
1.4.1.2.1. Disposiciones Generales sobre Activos de Información				
.1	La Dirección de Proveeduría es encargada de la realizar el proceso de compra de los activos informáticos de acuerdo a las solicitudes de compra de bienes y servicios generadas por las diferentes dependencias, las cuales deben contar con el visto bueno de la DGTI, una vez que recibe los activos en el Almacén se los traslada a los Encargados de Control de Bienes e Inventarios. Por otro lado, la Dirección de Control de Bienes e Inventarios lleva a cabo el plaqueo, la asignación y entrega del equipo al usuario final, por medio del Formulario de Asignación de Activos	**SÍ**	El coordinador de Sede se encarga antes de entregarse el equipo al usuario final, de probar y configurar el equipo antes de ser entregado a la dependencia solicitante	
.2	El personal de Gestión Técnica realiza la instalación del equipo, así como asigna una contraseña temporal, que deberá ser cambiada por el usuario periódicamente.	**SÍ**	El coordinador de Sede configurar el usuario en el equipo de la persona que lo utilizara una vez entregado a la dependencia solicitante	

1.4.1.2.1.2. Uso de los Activos Informáticos				
.1	El personal de Seguridad de la Información debe establecer los lineamientos para la protección de los datos almacenados y gestionados por medio de recursos de TI (internet, correo electrónico, computadoras, dispositivos móviles, servidores, impresoras). P	**NO APLICA**		
.2	El usuario es el responsable final de la protección de los datos contenidos en los activos informáticos que utiliza, según los lineamientos de seguridad que han sido establecidos y lo indicado en el Artículo 4 del Reglamento de Control de Bienes de la UTN.	**NO**	en sede la información es almacenada correspondiente al servidor de archivos, los cuales solo tiene accesos el personal responsable de cada unidad	
.3	El equipo debe bloquearse y protegerse cuando se deje sin supervisión, evitando que personas externas puedan acceder a la información.	**SÍ**	el equipo se bloquea transcurrido cierto tiempo de no utilizarse.	
.4	El equipo y los sistemas de la Universidad Técnica Nacional deben emplearse sólo para los fines autorizados por la institución.	**SÍ**		
.5	Los medios de almacenamiento de datos utilizados para el trabajo fuera de la oficina deben recibir el mismo nivel de protección física que el almacenamiento *in situ*.	**SÍ**		
.6	Deben implementarse los requerimientos de seguridad respectivos en el desarrollo de aplicaciones e instalación de equipo (hardware), previo a su integración a la plataforma tecnológica de UTN.	**NO APLICA**		
.7	Las contraseñas y accesos a los sistemas deben ser de conocimiento personal y único de los funcionarios que han sido autorizados para su uso. Por ello, no debe mantenerse esta información en lugares visibles, donde pueda ser vista por otras personas.	**SÍ**		
.8	El usuario es el responsable final de resguardar la integridad física del equipo que utiliza, siguiendo las normas generales de uso de equipo informático, según el tipo activo.	**SÍ**		
1.4.1.2.2. Disposiciones Generales de Seguridad				

.1	Los dueños de la información (establecidos en el Diccionario de Datos Empresarial), deben asegurar que los datos bajo su responsabilidad se encuentren identificados y clasificados. De igual forma, es su responsabilidad definir la criticidad y sensibilidad de la información, con el objetivo, de que se apliquen los debidos niveles de seguridad para la protección de la integridad y confidencialidad de la información.	**NO APLICA**		
.2	Todo funcionario de la Universidad Técnica Nacional debe eliminar aquella información electrónica que el área de la institución ya no requiera y que no se encuentre sujeta a ningún requerimiento de retención, según lo establecido por el Comité Institucional de Selección y Eliminación de Documentos. Seguidamente, la jefatura debe entregar el dispositivo de almacenamiento electrónico al personal de la Gestión Técnica de la DGTI para su eliminación segura siguiendo el proceso requerido, ya sea reciclar, reasignar, reutilizar o desechar.	**SÍ**		
.3	De igual forma, la información clasificada como Interna y Restringida en formato físico, deberá eliminarse siguiendo los lineamientos establecidos, incluyendo aquellos datos almacenados en formato físico (ej. contratos en papel, CDs, DVDs, unidades USB), siempre y cuando no sean requeridos por la UTN y no tengan ningún requerimiento de retención.	**NO**		
.4	se aplica enmascaramiento de datos, con el objetivo de mantener el anonimato de información sensible ante posibles accesos no autorizados por usuarios externos y/o internos de la institución.	**NO APLICA**		

.5	Se solicita por parte de los dueños de los datos el enmascaramiento de la información, según la criticidad y sensibilidad, valorando los casos en que la confidencialidad de la información de los estudiantes o funcionarios pueda verse amenazada, en especial cuando la información es compartida a terceros.	**NO APLICA**		
.6	Se realiza reemplazando información de carácter sensible por datos aleatorios, que permita al personal de desarrollo realizar las pruebas técnicas, sin acceder a información real de los funcionarios y/o estudiantes	**NO APLICA**		

OBJETIVO:

Verificar el cumplimiento de la normativa de TI, su adecuada Aplicación.

EXPLICACIÓN DE MARCAS:

Sí = Prueba Satisfactoria
NO = Prueba insatisfactoria
NO APLICA = No se evalúa el enunciado ya que no puede ponerse en práctica de la sede en estudio.

OBSERVACIONES:

a. Muchos de los archivos no se han actualizado desde el 2016

b. Algunos archivos como reglamentos que habla en la Normativa NO se encuentran en la información brindada.

CONCLUSIÓN:

De acuerdo con los procedimientos realizados, se concluye que existe una adecuada administración de los dispositivos de control ambiental pero dicho proceso es llevado a cabo por el coordinador de sede y no por el personal de seguridad.

EVALUACIÓN DE NORMATIVA 1.4. Gestión de la Seguridad de la Información Aplicada en UTN Sede Pacífico: 1.4.2. Compromiso del Personal con la Seguridad de la Información	REF:	HT-02
	Hecho por:	JAHG
	Fecha:	1-May-18
	Revisado por:	
	Fecha:	

ÍTEM	PREGUNTA	Aplicación	JUSTIFICACIÓN	EVIDENCIAS
.1	Existe políticas, normativas existentes acerca de Compromiso del Personal con la Seguridad de la Información	NO APLICA	En la normativa no existe nada referente a Compromiso del Personal con la Seguridad de la Información	

OBJETIVO:

Verificar el cumplimiento de la normativa de TI, su adecuada Aplicación en la sede.

EXPLICACIÓN DE MARCAS:

Sí = Prueba Satisfactoria
NO = Prueba insatisfactoria
NO APLICA = No se evalúa el enunciado ya que no puede ponerse en práctica de la sede en estudio.

OBSERVACIONES:

a. Muchos de los archivos de la normativa no se han actualizado desde el 2016

b. Algunos archivos como reglamentos que habla en la Normativa NO se encuentran en la información brindada.

CONCLUSIÓN:

De acuerdo con los procedimientos realizados, se concluye que existe una adecuada administración de los dispositivos de control ambiental.

EVALUACIÓN DE NORMATIVA 1.4. Gestión de la Seguridad de la Información Aplicada en UTN Sede Pacífico: 1.4.3. Seguridad Física y Ambiental	REF:	HT-03
	Hecho por:	JAHG
	Fecha:	1-May-18
	Revisado por:	
	Fecha:	

ÍTEM	PREGUNTA	Aplicación	JUSTIFICACIÓN	EVIDENCIAS
1.4.3.1. DGTI-PO-3300020 Procedimiento Acceso a Instalaciones Restringidas de TI.				
1.4.3.1.1. Control de Visitantes a Instalaciones Restringidas de TI				
.1	El visitante (funcionario de la UTN, proveedor o personal de emergencias) solicita acceso al Jefe de Gestión Técnica, indicando: el motivo de la visita, quienes ingresarán, el período de tiempo y cualquier otro aspecto que considere necesario.	SÍ	En sede el visitante se presenta con el guarda e indica con la persona que desea hablar o la persona que lo espera, el guarda procede a registrarlo en bitácora de visita y también registra si trae equipo, además de comunicar a la personal que el visitante se encuentra en la puerta	
.2	El Jefe de Gestión Técnica valora si responde a una emergencia la solicitud de ingreso.	SÍ	guarda de seguridad de la sede llama al personal que llego el visitante.	
.3	El Jefe de Gestión Técnica valora la aprobación de la solicitud. De negativo se le notifica al visitante las razones por las cuales le fue negada su solicitud, y se da fin a este procedimiento.	NO APLICA	Correspondientes a Visitas de TI, proveeduría, aprovisionamiento, jefatura le informan al coordinador mediante correo o llamada que en los próximos días estará visitando el personal de una empresa o el mismo personal de UTN, en caso de otras visitas si el personal se encuentra se procede a pasar la visita en caso contrario se procede a indicar que el personal no se encuentra.	

.4	El Jefe de Gestión Técnica designa a un funcionario de Infraestructura o coordinador de sede, quien en caso necesario será el encargado de custodiar la visita a la instalación.	SÍ	El jefe de Gestión Técnica informa a el coordinador de Sede y este se encarga de recibir al visitante.	
.5	Para la visita, Gestión Técnica verifica la necesidad de guía por parte del funcionario designado.	NO APLICA	En sede el visitante se presenta con el guarda e indica con la persona que desea hablar o la persona que lo espera, el guarda procede a registrarlo en bitácora de visita y también registra si trae equipo, además de comunicar a la personal que el visitante se encuentra en la puerta	
.6	El funcionario designado acompaña, sirviendo de guía durante la visita para que se cumplan los objetivos de la misma.	SÍ		
.7	El visitante (funcionario de la UTN, proveedor o personal de emergencias) lleva a cabo la visita.	SÍ		
.8	Cuando finaliza la visita se le solicita su registro en la bitácora de acceso (DGTI-FO-33000201 Formulario Bitácora de Visitantes a Instalaciones Restringidas de TI) y se completan los campos de control, para que luego se retiren del lugar. El funcionario designado deberá registrar la hora de salida.	SÍ		
1.4.3.2. DGTI-PO-3300030 Procedimiento Monitoreo del Ambiente Físico.				
1.4.3.2.1. Monitoreo de instalaciones restringidas de TI				
.1	El Jefe de Gestión Técnica designa el funcionario de infraestructura o coordinador de sede encargado de realizar el monitoreo del ambiente físico en las instalaciones restringidas de TI.	SÍ		
.2	El funcionario designado verifica como mínimo las condiciones ambientales de: humedad, UPS, aire acondicionado, energía, cableado estructurado, medidas ante desastres, estado de equipo, y cualquier otro requerimiento, según las características de las	SÍ	El Coordinador de Sede se encarga informar a las unidades de cualquier fallo con los equipos ya se ha aire, equipos, energía , estado de equipo mediante informes técnicos, boletas de mantenimiento o mediante llamadas a soporte externo	

	instalaciones restringidas.		si equipo cuenta con garantía.	
.3	El funcionario designado completa el DGTI-FO-33000301 Formulario Bitácora de Monitoreo del Ambiente Físico, con los hallazgos identificados.	SÍ		
.4	En caso de identificarse desviaciones, el funcionario designado debe comunicarlas a la Jefatura de Gestión Técnica para su atención y envía formulario al Jefe de Gestión Técnica.	SÍ	El coordinador emite informes técnicos según corresponda o bien se encarga de comunicar al jefe de Gestión Técnica	
.5	El Jefe de Gestión Técnica analiza la situación, según la información presentada en el formulario.	SÍ	El jefe de gestión técnica se encarga de brindar toda la ayuda posible según la situación presentada	
.6	El Jefe de Gestión Técnica define las actividades a ejecutar para cubrir las desviaciones identificadas, así como el personal encargado de ejecutarlas.	SÍ		
.7	El personal designado lleva a cabo las tareas que han sido definidas por la Jefatura de Gestión Técnica, generando la documentación necesaria que sirva como evidencia de la ejecución de las mismas.	SÍ		
.8	El Jefe de Gestión Técnica verifica que el personal designado haya realizado las tareas indicadas previamente, valorando los resultados obtenidos.	SÍ	el jefe de gestión técnica revisa continuamente los casos que se le comunican en la página de soporte	
1.4.3.2.2. Revisión de accesos				
.1	El personal de Seguridad de la Información realiza una visita a las instalaciones protegidas y visualiza las medidas tomadas para el acceso de personal a estas zonas.	SÍ	UTN no cuenta con personal de seguridad, El coordinador de sede se encarga de realizar visitas a las instalaciones	
.2	El personal de Seguridad de la Información solicita evidencia de las bitácoras de acceso del último trimestre a la Jefatura de Gestión Técnica.	NO	Aun no se han solicitado las bitácoras de acceso.	

.3	El Jefe de Gestión Técnica reúne la evidencia de las bitácoras de acceso del último trimestre.	NO	Aun no se han solicitado las bitácoras de acceso.	
.4	El Jefe de Gestión Técnica envía la evidencia de las bitácoras de acceso al responsable de Seguridad de la Información. Nota: De haberse identificado un incidente en el acceso por parte del personal de infraestructura, el Jefe de Gestión de Técnica debe comunicarlo al responsable de Seguridad de la Información.	NO APLICA	UTN no cuenta con personal de seguridad,	
.5	El responsable de Seguridad de la Información selecciona una muestra de la evidencia enviada.	SÍ	el jefe de gestión técnica revisa continuamente los casos que se le comunican en la página de soporte	
.6	El responsable de Seguridad de la Información analiza la muestra seleccionada, verificando que se hayan cumplido los requerimientos de control de acceso a las instalaciones restringidas de TI.	SÍ	el jefe de gestión técnica revisa continuamente los casos que se le comunican en la página de soporte	
.7	En caso de identificarse desviaciones, el responsable de Seguridad de la Información deberá generar un informe que describa las acciones a realizar para el cierre de las brechas identificadas.	NO	el Coordinador de Sede se encarga de comunicar mediante informe Técnico al jefe de Gestión Técnica	
.8	El responsable de Seguridad de la Información valora si se ha producido un incidente de seguridad. De ser así, se ejecuta el DGTI-PO-3300040 Procedimiento Gestión de Incidentes de Seguridad. De lo contrario, se tratará como un evento, y se proseguirá con el siguiente paso de este procedimiento.	SÍ	el jefe de gestión técnica revisa continuamente los casos que se le comunican en la página de soporte	
.9	El responsable de Seguridad de la Información comparte el informe desarrollado al Comité de Seguridad de la Información, para la valoración de las actividades a ejecutar.	NO APLICA		
1.4.3.2.3. Revisión de monitoreo y mantenimientos				

.1	El responsaB42:D48za una visita a las instalaciones de TI, evaluando el estado del equipo en conjunto con el Jefe de Gestión Técnica. Nota: Utiliza como base el DGTI-FO-33000301 Formulario Bitácora de Monitoreo de Ambiente Físico.	NO	No se cuenta con responsable de Seguridad de TI	
.2	El responsable de Seguridad de la Información solicita evidencia (Bitácoras de Monitoreo de Ambiente Físico y Plan de Mantenimiento y Adquisición) a la Jefatura de Gestión Técnica sobre los monitoreo y mantenimientos realizados en el último trimestre.	NO		
.3	El Jefe de Gestión Técnica reúne la evidencia acerca de los monitoreo y mantenimientos realizados. Nota: Debe tomarse en cuenta las actividades de mantenimiento definidas en el "DGTI-FO 34000501 Formulario Plan de Adquisición y Mantenimiento de Infraestructura".	NO APLICA		
.4	El Jefe de Gestión Técnica envía la información recolectada (evidencia de monitoreo y mantenimiento) al responsable de Seguridad de la Información.	NO APLICA		
.5	El responsable de Seguridad de la Información selecciona una muestra de la información enviada para su revisión.	NO APLICA		
.6	El responsable de Seguridad de la Información evalúa la muestra seleccionada, y verifica que efectivamente se realicen los monitoreo y mantenimientos de las instalaciones de TI.	NO APLICA		
.7	En caso de identificarse desviaciones, el responsable de Seguridad de la Información deberá generar un informe que describa las acciones a realizar y será entregado al personal responsable.	NO APLICA		

.8	El responsable de Seguridad de la Información valora si se ha producido un incidente de seguridad y procede en registrarlo en DGTI-PO-3300040 Procedimiento Gestión de Incidentes de Seguridad.	NO APLICA		
.9	El responsable de Seguridad de la Información envía el informe al Comité de Seguridad de la Información, para la valoración de las actividades a ejecutar.	NO APLICA		
1.4.3.3. DGTI-PO-5305010 Procedimiento Desecho y Reutilización de Equipo de TI.				
1.4.3.3.1. Reutilización del Equipo de TI				
.1	Se genera una solicitud de cambio de equipo de TI por medio de la mesa de servicio.	SÍ	En sede el personal que requiera cambio de equipo ya sea por daño o por obsolescencia debe solicitar un informe técnico al Coordinador de sede donde se hace constar la situación del Equipo, luego se encarga de realizar la solicitud mediante el sitio web avatar, guiado por el manual de equipo,	
.2	El funcionario de Soporte designado, realiza el cambio del equipo.	NO APLICA	Una vez adquirido el equipo y entregado por activos fijos al interesado, debe solicitar al coordinador de sede mediante mesa de trabajo la solicitud del cambio del equipo,	
.3	El funcionario responsable del activo traslada el equipo antiguo a la DGTI, para lo cual utiliza la Boleta de Traslado de Activos de la Dirección de Control de Bienes.	NO APLICA	el funcionario encargado de activos transfiere al Coordinado de sede el activo mediante la boleta de traslado si el activo se pudiese utilizar, pero si el activo no se puede utilizar deberá ser enviado a Activos para ser dado de baja mediante un informe técnico y mediante la boleta de desincorporación.	
.4	El funcionario de Soporte lleva a cabo un formateo del equipo, eliminando la información contenida en él.	NO APLICA	En sede no se cuenta con funcionario de soporte por lo el coordinador de sede encarga de instalar y configurar el equipo	

.5	El funcionario de soporte almacena el equipo y valora las opciones de transferencia del equipo cuando el Área de Gestión Técnica lo determina, realiza la gestión para su traslado, por medio de la Boleta de Traslado de Activos de la Dirección de Control de Bienes.	NO APLICA	El encargado de activos se encarga de reubicar los activos aun funcionales	
1.4.3.3.2. Desecho del Equipo de TI				
.1	Un funcionario genera una solicitud de desecho de equipo por medio de la mesa de servicio.	SÍ	Los funcionarios reportan mediante mesa de trabajo y El coordinador de sede toma el caso de la mesa de trabajo y se encarga de realizar las pruebas necesarias sobre el activo y genera el informe técnico para que se proceda como corresponde.	
.2	El funcionario de Soporte procede con la revisión del equipo, verificando el tipo y estado.	NO	El coordinador de sede y se encarga de realizar las pruebas necesarias sobre el activo y genera el informe técnico para que se proceda como corresponde.	
.3	El funcionario de soporte emite un Informe Técnico detallando las características del equipo y la razón por la cual se da de baja técnicamente.	NO		
.4	En caso que sea un equipo de almacenamiento se procede con el procedimiento DGTI-PO-5306010 Manejo de Medios de Almacenamiento.	NO	EL coordinador de sede toma el caso, y procede con realizar los respaldos necesarios y realizar el borrado de bajo nivel	
.5	El usuario solicitante entrega el activo junto con el Informe Técnico recibido a la Dirección de Control de Bienes e Inventarios (DCBI), que procede según el procedimiento definido.	SÍ	El solicitante procede con la entrega del activo mediante la boleta de respectiva y con copia del informe técnico.	

OBJETIVO:

Verificar el cumplimiento de la normativa de TI en lo que ha Seguridad Física y Ambiental se refiere, su adecuada Aplicación.

EXPLICACIÓN DE MARCAS:

Sí = Prueba Satisfactoria

NO = Prueba insatisfactoria

NO APLICA = No se evalúa el enunciado ya que no puede ponerse en práctica de la sede en estudio.

OBSERVACIONES:

a. En sede no se cuenta con personal de soporte, quien se encarga de ellos es el coordinador de TI.
b. Algunos archivos como reglamentos que habla en la Normativa NO se encuentran en la información brindada.

CONCLUSIÓN:

De acuerdo con los procedimientos realizados, se concluye que existe una adecuada administración de los dispositivos de control ambiental.

EVALUACIÓN DE NORMATIVA 1.4. Gestión de la Seguridad de la Información Aplicada en UTN Sede Pacífico: 1.4.4. Seguridad en las operaciones y comunicaciones	REF:	HT-04
	Hecho por:	JAHG
	Fecha:	1-May-18
	Revisado por:	
	Fecha:	

ÍTEM	PREGUNTA	Aplicación	JUSTIFICACIÓN	EVIDENCIAS
1.4.4.1. DGTI-PO-3300040 Procedimiento Gestión de Incidentes de Seguridad.				
1.4.4.1.1. Detección de Incidentes de Seguridad				
.1	El responsable de Seguridad de la Información recibe un reporte vía mesa de servicios, que describe la detección de un incidente de seguridad de la información, el cual puede ser originado desde las siguientes fuentes: Por un usuario desde la Mesa de Servicio. Por el responsable de Seguridad de la Información mediante monitoreo de rutina o denuncias directas de los usuarios. Por un sistema o herramienta automatizada de detección y protección.	NO APLICA		
.2	El responsable de Seguridad de la Información revisa el reporte y ejecuta el sub procedimiento de valoración de incidentes de seguridad (paso 8.2), con el objetivo de determinar si efectivamente se trata de un incidente de seguridad o es solamente un evento.	NO APLICA		
.3	En caso de ser un incidente, proseguir con el subprocedimiento Atención de Incidente (8.3). De lo contrario, se notifica a quien envió el reporte, que se trata de una falsa alarma.	NO APLICA		

1.4.4.1.2. Valoración de Incidentes de Seguridad				
.1	El responsable de Seguridad de la Información analiza el riesgo que presenta el incidente, para lo cual valora su impacto y urgencia.	**NO APLICA**		
.2	El responsable de Seguridad identifica si hay repercusiones en TI, de ser así contacta al funcionario especialista en el área de impacto. De lo contrario, se sigue con el paso 8.2.4	**NO APLICA**		
.3	El especialista de TI brinda asesoría en la valoración del riesgo que presenta el incidente de seguridad para la Institución.	**NO APLICA**		
.4	Con base en el análisis llevado a cabo, el responsable de Seguridad de la Información define si se trata o no, de un incidente de seguridad de la información.	**NO APLICA**		
1.4.4.1.3. Atención de Incidentes de Seguridad				
.1	El responsable de Seguridad de la Información analiza las actividades a ejecutar para la atención del incidente, con el objetivo de identificar su causa raíz.	**NO APLICA**		
.2	Si la complejidad del incidente requiere de apoyo interdisciplinario, el responsable de Seguridad de la Información solicita una sesión de emergencia del CSI, involucrando al personal de las áreas afectadas.	**NO APLICA**		
.3	Con base en el análisis, el CSI junto con el responsable de Seguridad de la Información determina las actividades a ejecutar para dar respuesta al incidente.	**NO APLICA**		

.4	El responsable de Seguridad de la Información define en conjunto con las jefaturas quien es el funcionario o grupo de funcionarios encargados de llevar a cabo las actividades y genera el caso respectivo en la mesa de servicios. Nota: Según el tipo de incidente, el responsable de Seguridad de la Información debe formar parte del grupo encargado de dar respuesta al incidente.	**NO APLICA**		
.5	El funcionario o grupo de funcionarios llevan a cabo las tareas para mitigar el riesgo asociado al incidente de seguridad. Nota: **En caso que el incidente, requiera un cambio sobre un módulo, aplicación, sistema o solución, tomar en cuenta también el Procedimiento DGTI-PO-5200010 Gestión de Cambios (Software).**	**NO APLICA**		
1.4.4.1.4. Seguimiento y Cierre de Incidentes de Seguridad				
13	El responsable de Seguridad de la Información da seguimiento a la ejecución de las actividades.	**NO APLICA**		
14	En caso de identificar desviaciones entre lo planificado y lo realizado, el responsable de Seguridad de la Información determina las medidas a tomar, que permitan dar una efectiva respuesta al incidente presentado.	**NO APLICA**		
15	Funcionario o grupo de funcionarios ejecuta acciones de respuesta y se genera un informe técnico que se traslada al responsable de Seguridad de la Información, con el detalle de la solución, quien lo almacena para sucesos futuros.	**NO APLICA**		

16	El responsable de Seguridad de Información verifica que efectivamente se haya solucionado el incidente. De ser así, se da cierre al incidente de seguridad, de lo contrario, se devuelve al subprocedimiento Atención de Incidentes, con el objetivo de definir las tareas a realizar.	**NO APLICA**		
1.4.4.1.5. Evaluación de Incidentes de Seguridad				
.1	El responsable de Seguridad de la Información mensualmente analiza la información de los incidentes de seguridad que han representado un riesgo mediano o grande, utilizando para ello el DGTI-FO-12000101 Formulario Valoración de Riesgos. En caso de no haberse presentado, incidentes de este tipo en el mes, se finaliza este procedimiento.	**NO APLICA**		
.2	El responsable de Seguridad de la Información valora las lecciones aprendidas en la detección, atención, respuesta y cierre de los incidentes de seguridad presentados en el mes anterior.	**NO APLICA**		
.3	El responsable de Seguridad de la Información presenta las lecciones aprendidas que son derivadas de los incidentes de seguridad, en la sesión del CSI.	**NO APLICA**		
.4	Los miembros del CSI determinan si es necesario realizar actividades posteriores (por ejemplo, capacitaciones) que eviten la recurrencia de los incidentes de seguridad identificados, de ser así las definen. De no identificarse actividades, se da por finalizado este procedimiento.	**NO APLICA**		

.5	El responsable de Seguridad de la Información lleva a cabo las tareas que han sido definidas en la sesión del CSI.	**NO APLICA**		
.6	El responsable de Seguridad de la Información notifica al CSI sobre los resultados obtenidos de las actividades.	**NO APLICA**		
1.4.4.2. DGTI-PO-5100020 Procedimiento Protección contra Software Malicioso.				
1.4.4.2.1. Prevención y Detección de Software Malicioso				
.1	La jefatura de Gestión Técnica designa un funcionario de Infraestructura encargado de revisar periódicamente el equipo contra software malicioso.	**NO APLICA**		
.2	El técnico de Infraestructura designado procede con la extracción de reportes de las herramientas utilizadas para la prevención y detección de software malicioso.	**NO APLICA**		
.3	El técnico de Infraestructura revisa los reportes, valorando si se ha presentado algunas de las siguientes situaciones:	**NO APLICA**		
.4	Detección de software malicioso en la red universitaria.	**NO APLICA**		
.5	Detección de actividades que incumplen con las políticas de seguridad informática de la UTN.	**NO APLICA**		
.6	De darse alguna de estas situaciones, se generan solicitudes de incidentes, ejecutando el procedimiento DGTI-PO-3300040 Procedimiento Gestión de Incidentes de Seguridad. De lo contrario, se prosigue con el paso 8.1.6.	**NO APLICA**		

.7	Una vez que los incidentes han sido atendidos y solucionados, el técnico de Infraestructura valora si debe realizarse un cambio en la configuración de los sistemas de prevención y detección de software malicioso. De ser así, se ejecuta el DGTI-PO-5111010 Procedimiento Gestión de Cambios (TI), y posteriormente se continúa .	**NO APLICA**		
.8	El técnico de Infraestructura lleva a cabo un informe de gestión de los sistemas de detección y prevención de software malicioso, detallando los hallazgos identificados durante la revisión y las actividades realizadas.	**NO APLICA**		
.9	El técnico de Infraestructura envía el informe al personal de Seguridad de la Información y la Jefatura de Gestión Técnica, para su respectiva valoración.	**NO APLICA**		
1.4.4.3. DGTI-PO-5107010 Procedimiento Gestión de Respaldos y Restauraciones.				
1.4.1.1.1. Solicitud de Respaldo				
.1	El interesado genera una solicitud vía mesa de servicio para el respaldo de información, la cual puede ser derivada de un requerimiento universitario, o bien, por una necesidad de Continuidad de TI para el respaldo de información crítica. Nota: **Las solicitudes pueden ser recurrentes o no recurrentes.**	**SÍ**	Coordinador de sede se encarga de procesar la acción solicitada sobre la el respaldo del usuario solicitado	
.2	El Administrador de Respaldos revisa la calendarización establecida, verifica la fecha de la solicitud recibida y la programa según la prioridad y urgencia.	**SÍ**		

.3	El Técnico de Infraestructura asignado (según mesa de servicio) verifica el estado del medio de almacenamiento donde se realizará el respaldo. Si el medio de almacenamiento está próximo a vencer o se encuentra en mal estado, se procede con el DGTI-PO-5306010 Procedimiento Tratamiento de Medios de Almacenamiento, **y el Técnico de Infraestructura utilizará un nuevo medio.**	**SÍ**		
.4	El Técnico de Infraestructura procede con el respaldo de la información, siguiendo el protocolo definido.	**NO APLICA**		
.5	El Técnico de Infraestructura verifica si el respaldo fue exitoso.	**NO APLICA**		
.6	El Técnico de Infraestructura verifica que el respaldo cuente con los requerimientos de seguridad, bloqueando los permisos de escritura.	**NO APLICA**		
.7	El Técnico de Infraestructura comunica al Interesado sobre la finalización del respaldo.	**NO APLICA**		
1.4.1.1.2. Solicitud de Restauración				
.1	El interesado de la información o encargado de Continuidad de TI solicita una restauración por medio de la mesa de servicio.	**SÍ**		
.2	El Técnico de Infraestructura (asignado según mesa de servicio) analiza la solicitud, y compara la antigüedad de la información con los requerimientos de retención. En caso de no proceder el requerimiento, se comunica al interesado y se finaliza el proceso. De lo contrario, continua con el paso 8.2.3.	**SÍ**		

.3	El Administrador de Respaldos analiza la solicitud y establece la fecha de la restauración, según la prioridad y urgencia de la misma.	**SÍ**		
.4	El Técnico de Infraestructura procede con la restauración de la información.	**SÍ**		
.5	El Técnico de Infraestructura verifica si la restauración fue exitosa. De ser así, continúa con la actividad 8.2.6, de lo contrario, regresa al paso 8.2.4.	**SÍ**		
.6	El Técnico de Infraestructura coloca la información en la ubicación o ambiente requerido.	**SÍ**		
.7	El Técnico de Infraestructura comunica los resultados al Interesado por medio de la mesa de servicio, de modo que este verifique si la información es íntegra.	**SÍ**		
.8	El Interesado analiza la información y comunica el resultado.	**SÍ**		
.9	En caso que la información restaurada no sea íntegra, se procederá con el paso 8.2.4. De lo contrario, se da por finalizado este procedimiento.	**SÍ**		
1.4.1.1.3. Pruebas de Respaldos y Restauraciones				
.1	El Administrador de Respaldos establece en conjunto con la Jefatura del Área de Gestión Técnica, el calendario para realizar pruebas de restauración y respaldo.	**NO APLICA**	Coordinador de sede se encarga de procesar la acción solicitada sobre la el respaldo del usuario solicitado	
.2	El Técnico de Infraestructura designado (según la mesa de servicios),será el encargado de la ejecución de pruebas.	**NO APLICA**		
.3	El Técnico de Infraestructura selecciona los respaldos de la fecha establecida, designados para realizar la prueba.	**NO APLICA**		
.4	El Técnico de Infraestructura realiza la restauración sobre los respaldos seleccionados.	**NO APLICA**		

.5	En caso de presentarse un error, el Técnico de Infraestructura reporta la prueba como fallida al Administrador de Respaldos y finaliza el procedimiento. De lo contrario, sigue con el paso 8.3.6.	**NO APLICA**		
.6	El Técnico de Infraestructura sube la información al servidor de restauraciones.	**NO APLICA**		
.7	El Técnico de Infraestructura comunica al Interesado que verifique si la información ha sido restaurada correctamente, indicando la ubicación definida para las pruebas.	**NO APLICA**		
.8	El Interesado analiza la información y comunica los resultados obtenidos.	**NO APLICA**		
.9	Si la información restaurada no es íntegra, el Técnico de Infraestructura reporta la prueba como fallida, y realiza las actividades necesarias para su solución.	**NO APLICA**		
.10	De lo contrario, reporta la prueba como exitosa al Administrador de Respaldos. En ambos casos, se debe adjuntar la evidencia respectiva y dar por finalizado el proceso.	**NO APLICA**		
1.4.4.4. DGTI-PO-5406010 Procedimiento Tratamiento de Medios de Almacenamiento.				
1.4.1.2.1. Eliminación de Datos				
.1	El Administrador de Respaldos ingresa una solicitud para la eliminación de datos por medio de la Mesa de Servicio.	**NO APLICA**	Coordinador de sede se encarga de procesar la acción solicitada sobre la el respaldo del usuario solicitado	
.2	El Técnico Especialista verifica la antigüedad de los datos, comparando la fecha en que fueron respaldados, y los requerimientos de retención establecidos por Archivo Institucional.	**NO APLICA**		

.3	En caso de no identificarse respaldos por eliminar, el Técnico Especialista comunica los resultados del monitoreo al Administrador de Respaldos, y el procedimiento finaliza.	**NO APLICA**		
.4	El Técnico Especialista selecciona los medios de almacenamiento que según los requerimientos de retención, contienen información que debe ser eliminada.	**NO APLICA**		
.5	El Técnico comunica los datos que serán eliminados, a la Jefatura de Gestión Técnica y la DGTI, para su respectiva validación. De darse la aprobación, sigue con el paso 8.1.6. De lo contrario, se comunica al Administrador de Respaldos y el proceso se da por finalizado.	**NO APLICA**		
.6	El Técnico Especialista procede con el borrado de la información.	**NO APLICA**		
.7	El Técnico Especialista verifica que el borrado se haya realizado correctamente.	**NO APLICA**		
.8	En caso que el medio de almacenamiento quede vacío, se procede con su formateo a bajo nivel. De lo contrario, se da por finalizado el procedimiento y se notifica al Administrador de Respaldos sobre los resultados encontrados.	**NO APLICA**		
1.4.1.2.2.	**Destrucción de Medios de Almacenamiento**			
.1	El Administrador de Respaldos ingresa una solicitud en la mesa de servicios para la destrucción de medios de almacenamiento y se designa al encargado del monitoreo.	**NO APLICA**	Coordinador de sede se encarga de procesar la destruir los medios de almacenamiento mediante de métodos a bajo nivel	
.2	El Técnico Especialista designado realiza un monitoreo de los medios de almacenamiento, verificando si hay equipos por destruir (caducados,	**NO APLICA**		

	están descontinuados o en mal estado).			
.3	En caso de no identificar medios por destruir, el Técnico Especialista notifica los resultados del monitoreo al Administrador de Respaldos y el procedimiento se da por finalizado. De lo contrario, continúa con el paso 8.2.4.	**NO APLICA**		
.4	El Técnico Especialista selecciona los medios que deben ser destruidos, según las condiciones mencionadas.	**NO APLICA**		
.5	El Técnico Especialista comunica a la Jefatura de Gestión Técnica y al Director de la DGTI, los medios que serán destruidos.	**NO APLICA**		
.6	La Jefatura de Gestión Técnica en conjunto con el Director de la DGTI valida la eliminación de los medios. De darse la aprobación, el Técnico Especialista elabora el acta de destrucción y se continúa con el paso 8.2.7, de lo contrario, se finaliza el procedimiento.	**NO APLICA**		
.7	El Técnico Especialista junto con otro funcionario de la DGTI, realiza la destrucción del medio.	**NO APLICA**		
.8	La Jefatura de Gestión Técnica envía una nota a la Dirección de Control de Bienes, notificando sobre la destrucción de medios y entrega los mismos para su baja administrativa.	**NO APLICA**		

OBJETIVO:
Verificar el cumplimiento de la normativa de TI, su adecuada Aplicación.

EXPLICACIÓN DE MARCAS:

Sí = Prueba Satisfactoria

NO = Prueba insatisfactoria

NO APLICA = No se evalúa el enunciado ya que no puede ponerse en práctica de la sede en estudio.

OBSERVACIONES:

a. Muchos de los archivos no se han actualizado desde el 2016

b. Algunos archivos como reglamentos que habla en la Normativa NO se encuentran en la información brindada.

CONCLUSIÓN:

De acuerdo con los procedimientos realizados, se concluye que existe una adecuada administración de los dispositivos de control ambiental.

EVALUACIÓN DE NORMATIVA 1.4. Gestión de la Seguridad de la Información Aplicada en UTN Sede Pacífico: 1.4.5. Control de Acceso	REF:	HT-05
	Hecho por:	JAHG
	Fecha:	1-May-18
	Revisado por:	
	Fecha:	

ÍTEM	PREGUNTA	Aplicación	JUSTIFICACIÓN	EVIDENCIAS
1.4.5.1.DGTI-PO-3300050 Procedimiento Control de Acceso.				
1.4.5.1.1.Creación de Cuentas de Dominio/Sistemas				
.1	La Dirección de Gestión de Desarrollo Humano o bien un funcionario interesado, genera una solicitud, mediante la mesa de servicio, para la creación de una nueva cuenta.	**SÍ**	Coordinador de sede se encarga de realizar la creación del usuario solicitado, y dar los accesos solicitado	
.2	El Administrador de Accesos, verifica que toda la información necesaria para procesar la solicitud esté presente o bien se solicita los datos faltantes.	**SÍ**		
.3	La jefatura inmediata del funcionario para quien se creará la cuenta, válida la solicitud. Si la aprueba, se continúa con el siguiente paso, de lo contrario, se notifica al solicitante y finaliza el procedimiento.	**SÍ**		
.4	El Administrador de Dominio o el Dueño del Sistema según corresponda, válida la creación de la cuenta. Si la aprueba, se continúa con el siguiente paso, de lo contrario, se notifica al solicitante y finaliza el procedimiento.	**SÍ**		
.5	El Administrador de Accesos, transfiere la solicitud para que un técnico de infraestructura la ejecute.	**NO APLICA**		

.6	El técnico de infraestructura, verifica que la cuenta no haya sido creada con anterioridad. Si no se ha creado, continúa con el siguiente paso, de lo contrario, se le notifica al solicitante, al Administrador de Accesos y el proceso finaliza.	**NO APLICA**		
.7	El técnico de infraestructura procede con la creación de la nueva cuenta. Esta se crea con un perfil acorde a las funciones del usuario y con una contraseña temporal que el usuario deberá cambiar cuando utilice la cuenta por primera vez.	**NO APLICA**		
.8	El técnico de infraestructura notifica al solicitante y al Administrador de Accesos y se finaliza el procedimiento.	**NO APLICA**		
1.4.5.1.2.Modificación de Cuentas				
.1	La Dirección de Gestión de Desarrollo Humano o bien un funcionario interesado, genera una solicitud, mediante la mesa de servicio, para la modificación de una cuenta. Por ejemplo, cuando un funcionario cambia a un rol con funciones distintas o se modifica alguna información del funcionario.	**NO APLICA**	Coordinador de sede se encarga de realizar la modificación del usuario solicitado.	
.2	El Administrador de Accesos, verifica que la información necesaria para procesar la solicitud esté presente.	**NO APLICA**		
.3	La jefatura inmediata del funcionario al que pertenece la cuenta, válida la solicitud. Si la aprueba, se continúa con el siguiente paso, de lo contrario, se notifica al solicitante y finaliza el procedimiento.	**NO APLICA**		
.4	El Administrador de Dominio o el Dueño del Sistema según corresponda, válida la modificación de la cuenta. Si la aprueba, se continúa con el siguiente paso, de lo contrario, se notifica al solicitante y finaliza el procedimiento.	**NO APLICA**		

.5	El Administrador de Accesos, transfiere la solicitud para que un técnico de infraestructura la ejecute.	**NO APLICA**		
.6	El técnico de infraestructura procede con la modificación de la cuenta en el Dominio o en el Sistema correspondiente ya sea para actualizar información o para asociar o desasociar roles.	**NO APLICA**		
.7	El solicitante verifica que la modificación se haya realizado correctamente, si es así, avanza al siguiente paso, de lo contrario regresa al paso 8.2.6.	**NO APLICA**		
.8	El técnico de infraestructura notifica al solicitante y al Administrador de Accesos y se finaliza el procedimiento.	**NO APLICA**		
1.4.5.1.3.Deshabilitar, Habilitar o Eliminar Cuentas				
.1	La Dirección de Gestión de Desarrollo Humano o bien el Administrador de Accesos, genera una solicitud, mediante la mesa de servicio, para deshabilitar o habilitar una cuenta. Esta solicitud aplica cuando un funcionario ingresa, sale temporal o definitivamente de la UTN o cuando regresa a la Institución.	**NO APLICA**		
.2	El Administrador de Accesos, verifica que toda la información necesaria para procesar la solicitud esté presente. Si es así continúa con el siguiente paso, de lo contrario se le notifica al solicitante y el proceso finaliza.	**NO APLICA**	Coordinador de sede se encarga de procesar la acción solicitada Deshabilitar, Habilitar o Eliminar Cuentas, del usuario solicitado	
.3	La jefatura inmediata del funcionario al que pertenece la cuenta, válida la solicitud. Si la aprueba, se continúa con el siguiente paso, de lo contrario, se notifica al solicitante y finaliza el procedimiento.	**NO APLICA**		
.4	El Administrador de Accesos, transfiere la solicitud para que un técnico de infraestructura la ejecute.	**NO APLICA**		

.5	Si la solicitud es de eliminación, se avanza hasta el paso 8.3.7. Si la solicitud es para deshabilitar o habilitar el acceso, continúa con el siguiente paso.	**NO APLICA**		
.6	El técnico de infraestructura procede a actualizar el estado de la cuenta como inactiva o activa en el Dominio y en todos los Sistemas de la UTN. Luego avanza hasta el paso 8.3.10.	**NO APLICA**		
.7	La jefatura inmediata del funcionario de la cuenta debe indicar si requiere o no, la recuperación de la información del usuario. Si requiere recuperación se avanza al paso siguiente, de lo contrario se realiza el paso 8.3.9.	**NO APLICA**		
.8	El técnico de infraestructura realiza el respaldo de la información almacenada por el usuario y hace entrega del mismo a la jefatura inmediata de la cuenta por eliminar.	**NO APLICA**		
.9	El técnico de infraestructura procede con la eliminación de la(s) cuenta(s) y los perfiles del funcionario en los Sistemas de la UTN. Luego procede con la eliminación de la cuenta de dominio del funcionario.	**NO APLICA**		
.10	Finalmente, se notifica a la DGDH, al Administrador de Accesos y a los dueños de los Sistemas involucrados y se finaliza el procedimiento.	**NO APLICA**		
1.4.5.1.4.Restablecer Contraseñas o Desbloquear Cuentas				
.1	Cualquier funcionario con una cuenta activa genera una solicitud, mediante la mesa de servicio, para el restablecimiento de su contraseña o desbloqueo de su cuenta. Esta solicitud puede efectuarse, ya sea por olvido de contraseña, porque la cuenta se ha bloqueado o por motivos de seguridad.	**NO APLICA**	Coordinador de sede se encarga de procesar la acción solicitada sobre la cuenta, del usuario solicitado	

.2	El Administrador de Accesos, verifica que toda la información necesaria para procesar la solicitud esté presente. Si es así, transfiere la solicitud para que un técnico de infraestructura la ejecute. En caso contrario, se le notifica al solicitante y el proceso finaliza.	**NO APLICA**		
.3	El técnico de infraestructura procede con el restablecimiento de la contraseña o desbloqueo de la cuenta, ya sea en el Dominio o en el Sistema correspondiente.	**NO APLICA**		
.4	El funcionario solicitante verifica que la contraseña se haya restablecido correctamente o que la cuenta ya no esté bloqueada, si es así, se notifica al Administrador de Accesos y se finaliza el procedimiento. En caso contrario, volver al paso 8.4.3	**NO APLICA**		
1.4.5.1.5.Monitoreo de Cuentas y Accesos				
.1	El Administrador de Accesos genera una solicitud, mediante la mesa de servicio, para realizar la revisión ya sea de Dominio o de Sistemas UTN.	**NO APLICA**	Coordinador de sede se encarga de procesar el monitoreo de las cuentas	
.2	El Técnico de Infraestructura analiza la solicitud, verificando si se trata de una revisión de Dominio o de Sistemas. En caso de tratarse de Dominio, debe continuar con el paso 8.5.3, de lo contrario, debe avanzar hasta el paso 8.5.6.	**NO APLICA**		
.3	El Técnico de Infraestructura solicita a la Dirección de Gestión de Desarrollo Humano la lista de funcionarios que han abandonado permanente o temporalmente la Institución en el último periodo.	**NO APLICA**		
.4	El Técnico de Infraestructura verifica que se haya eliminado o deshabilitado las cuentas del personal que se ha retirado de la UTN, según lo comunicado por la DGDH.	**NO APLICA**		

.5	En caso de identificarse desviaciones, el Técnico de Infraestructura procede con la deshabilitación/eliminación de las cuentas, ejecutando el subprocedimiento Deshabilitar, Habilitar o Eliminar Cuentas	**NO APLICA**		
.6	Si la solicitud es para revisión de perfiles asignados	**NO APLICA**		
.7	El Técnico de Infraestructura obtiene la lista de perfiles asignados a cada usuario en los Sistemas de información. Luego envía esta información al dueño de cada Sistema para que valide si está correcta.	**NO APLICA**		
.8	Cuando se obtiene el resultado de estas revisiones, el Técnico de Infraestructura revisa si existe algún hallazgo o desviación con los perfiles asignados	**NO APLICA**		
.9	El Técnico de Infraestructura obtiene las bitácoras de acceso a los Sistemas de la UTN. Luego envía esta información al dueño de cada Sistema para que valide si está correcta.	**NO APLICA**		
.10	Cuando se obtiene el resultado de estas revisiones, el Técnico de Infraestructura revisa si hay algún hallazgo o inconveniente con los accesos registrados, de ser así se ejecuta el DGTI-PO-3300040 Procedimiento Gestión de Incidentes de Seguridad y luego continúa. Si no existe desviación, continúa con el siguiente paso.	**NO APLICA**		
.11	Se notifica los resultados del monitoreo y de todas las acciones realizadas al Administrador de Accesos por medio de un informe técnico.	**NO APLICA**		

.12	El Administrador de Accesos remite el informe técnico al Responsable de Seguridad de la Información para su respectivo análisis, así como a la Jefatura de Gestión Técnica para su control; y se da por finalizado el proceso.	**NO APLICA**		

OBJETIVO:
Verificar el cumplimiento de la normativa de TI, su adecuada Aplicación.

EXPLICACIÓN DE MARCAS:

Sí = Prueba Satisfactoria
NO = Prueba insatisfactoria
NO APLICA = No se evalúa el enunciado ya que no puede ponerse en práctica de la sede en estudio.

OBSERVACIONES:
a. Muchos de los archivos no se han actualizado desde el 2016
b. Algunos archivos como reglamentos que habla en la Normativa NO se encuentran en la información brindada.

CONCLUSIÓN:
De acuerdo con los procedimientos realizados, se concluye que existe una adecuada administración de los dispositivos de control ambiental.

EVALUACIÓN DE NORMATIVA 1.4. Gestión de la Seguridad de la Información Aplicada en UTN Sede Pacífico: 1.4.6. Seguridad en la implementación y mantenimiento de Software e infraestructura Tecnológica	REF:	HT-06
	Hecho por:	JAHG
	Fecha:	1-May-18
	Revisado por:	
	Fecha:	

ÍTEM	PREGUNTA	Aplicación	JUSTIFICACIÓN	EVIDENCIAS
1.4.6.1.DGTI-PA-15 Política Contratación de Terceros				
1.4.6.1.1.Criterios y condiciones generales del proceso de compra				
.1	Se debe garantizar el cumplimiento de los principios de eficiencia, eficacia, publicidad, libre competencia, igualdad, buena fe, intangibilidad patrimonial de la actividad contractual según lo establecido por el Reglamento de Contratación Administrativa en el artículo 2.	**NO APLICA**		
.2	Todo proceso de contratación será realizado única y exclusivamente por el personal de la Dirección de Proveeduría Institucional desde el área de Contratación Administrativa.	**NO APLICA**		
.3	Para lo que corresponde a la celebración de contratos, la Universidad Técnica Nacional deberá firmar un acuerdo de confidencialidad, cuando así lo solicite la DGTI, alineado a la Política de Seguridad de la Información.	**NO APLICA**		
.4	Las adquisiciones y contrataciones, que se realicen, deben estar asociados a una partida presupuestaria que tenga reservado el contenido suficiente para hacer frente a las obligaciones derivadas del proceso y en cumplimiento con los requerimientos del portafolio de proyectos, planes de trabajo o actividades operativas institucionales.	**NO APLICA**		

.5	La valoración preliminar de los bienes de TI que se desean adquirir, serán realizadas por el personal de la Dirección de Gestión de TI, según lineamientos que dicte el Comité de Arquitectura de la Información.	**NO APLICA**		
.6	El Área de Gestión Estratégica debe llevar el control para la ejecución y cumplimiento del Plan de Inversiones de TI. Cualquier cambio necesario, debe ser solicitado por la dirección o vicerrectoría respectiva, o bien por la rectoría, para su aprobación.	**NO APLICA**		
.7	En lo que respecta al Plan de Inversión de TI, la Dirección de Gestión de TI, por medio del Área de Gestión Estratégica, valida anualmente la adquisición de equipo tecnológico solicitado por unidades ejecutoras.	**NO APLICA**		
.8	La unidad de Aprovisionamiento del Área de Gestión Estratégica es la única autorizada por la DGTI para emitir aprobaciones técnicas para la compra de activos y servicios tecnológicos.	**NO APLICA**		
.9	Toda renovación o reposición de equipo de cómputo debe contar con el visto bueno del área de Aprovisionamiento de la Dirección de Gestión de TI; además de la aprobación de la jefatura inmediata de la unidad solicitante.	**NO APLICA**		
.10	Las adquisiciones deben ser congruentes con la infraestructura y los estándares tecnológicos de la Universidad Técnica Nacional, previamente acordados y aprobados por la Dirección de Gestión de TI.	**NO APLICA**		
.11	Para la elaboración de contratos o carteles relacionados con tecnología de información, la Dirección de Proveeduría Institucional debe involucrar a la Dirección de Gestión de Tecnologías de la Información.	**NO APLICA**		

.12	Las adquisiciones de equipo informático por medio de caja chica, requerirán del visto bueno de la Unidad de Aprovisionamiento de la DGTI.	**NO APLICA**		
1.4.6.1.2.Criterios y condiciones generales del proceso de pago de facturas a proveedores				
.1	La presente política y sus lineamientos se aplican a todos los procesos de pago de facturas a proveedores de TI que se realicen en la Universidad Técnica Nacional.	**NO APLICA**		
.2	Los días establecidos para la entrega de los productos y la recepción de facturas correspondientes, serán determinados por la Dirección de Proveeduría.	**NO APLICA**		
.3	Las transferencias se realizan, de acuerdo con el horario establecido por la Dirección Financiera.	**NO APLICA**		
1.4.6.1.3.Formalización, modificación y cierre de contratos				
.1	La Dirección de Proveeduría realizará la formalización, modificación y cierre de contratos según el procedimiento establecido, en concordancia con la Ley de Contratación Administrativa y el Reglamento a la Ley de Contratación Administrativa.	**NO APLICA**		
.2	El cierre de los contratos se realizará por medio del recibido de satisfacción (oficio), de parte de la unidad ejecutora responsable.	**NO APLICA**		
1.4.6.1.4.Pago de Contratos				
.1	La autorización de los pagos establecidos en los contratos será responsabilidad de la Dirección de Gestión Financiera, previo a una verificación de cumplimiento por parte de la unidad ejecutora solicitante y el Informe Técnico de la unidad de Aprovisionamiento de TI.	**NO APLICA**		
1.4.6.1.5.Conflicto de Interés				

.1	Deberán abstenerse de participar en las decisiones de compra relacionadas con el proveedor, los colaboradores que tengan alguna relación patrimonial o de parentesco por consanguinidad o afinidad con alguno de sus socios o ejecutivos, según lo estipulado por la Ley de Contratación Administrativa.	**NO APLICA**		
1.4.6.1.6.Incumplimientos de Proveedores				
.1	La Dirección de Proveeduría deberá llevar el control y registro de los incumplimientos de los proveedores, analizando la evidencia enviada por la unidad ejecutora que permita la debida justificación de la inconformidad, ésta deberá ser incluida en el expediente.	**NO APLICA**		
.2	La Administración aplicará las multas y penalizaciones por incumplimientos del proveedor, según lo estipulado en los artículos 47 y 49 del Reglamento a la Ley de Contratación Administrativa.	**NO APLICA**		

OBJETIVO:

Verificar el cumplimiento de la normativa de TI, su adecuada Aplicación.

EXPLICACIÓN DE MARCAS:

Sí = Prueba Satisfactoria
NO = Prueba insatisfactoria
NO APLICA = No se evalúa el enunciado ya que no puede ponerse en práctica de la sede en estudio.

OBSERVACIONES:

a. Muchos de los archivos no se han actualizado desde el 2016
b. Algunos archivos como reglamentos que habla en la Normativa NO se encuentran en la información brindada.

CONCLUSIÓN:

De acuerdo con los procedimientos realizados, se concluye que existe una adecuada administración de los dispositivos de control ambiental.