UNIVERSIDAD DE COSTA RICA

RECTORÍA

Resolución R-102-2015

CIUDAD UNIVERSITARIA RODRIGO FACIO, San Pedro de Montes de Oca, a las 16 horas del día 18 de mayo del año dos mil quince, Yo, Henning Jensen Pennington, Rector de la Universidad de Costa Rica, en uso de las atribuciones que me confiere el Estatuto Orgánico y,

CONSIDERANDO:

1. La Contraloría General de la República emitió el documento de Directrices Técnicas para la Gestión y el Control de la Tecnologías de la Información (N-2-2007 CO-DFOE), relativo al fortalecimiento de la administración de los recursos públicos invertidos en Tecnologías de la Información y Comunicación (TIC).

2. Dicha normativa establece que el punto 1.4 Gestión de la seguridad de la información, que *"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales".*

   Para ello debe documentar e implementar Directrices técnicas de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:
   - La implementación de un marco de seguridad de la información.
   - El compromiso del personal con la seguridad de la información.
   - La seguridad física y ambiental.
   - La seguridad en las operaciones y comunicaciones.
   - El control de acceso.
   - La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
   - La continuidad de los servicios de TI.

   Además debe establecer las medidas de seguridad relacionadas con:
   - El acceso a la información por parte de terceros y la contratación de servicios prestados por estos.
   - El manejo de la documentación.
   - La terminación normal de contratos, su rescisión o resolución.
   - La salud y seguridad del personal.

75 ANIVERSARIO

Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados.

3. Que el Comité Gerencial de Informática, en sesión ordinaria Nº2-2014 Acuerdo 4.1, acordó enviar a la Rectoría el documento "Directrices de Seguridad de la Información" para su aprobación y que sea informado a la Comunidad Universitaria por medio de una resolución.

4. Que la Institución reconoce la importancia de adoptar un conjunto de Directrices Técnicas de Seguridad de Información, que además de tener como premisa básica la protección de la información perteneciente a la Universidad en su custodia, constituye el fundamento de la cultura que en materia de seguridad de la información desea establecer, reforzar, implementar e incorporar en su diario quehacer, con miras no sólo a lograr un manejo eficiente de sus recursos informáticos, acorde con el interés público y en estricta concordancia con el ordenamiento jurídico costarricense, sino sobre todo, a propiciar la eficiencia en las labores y el mejoramiento constante de los servicios que le dan fundamento a la Institución.

POR TANTO:

1. Apruebo las "Directrices de Seguridad de la Información de la Universidad de Costa Rica", que se adjunta a la presente resolución, cuya aplicación será obligatoria.

2. Corresponderá al Centro de Informática la ejecución de las labores necesarias para su implementación efectiva en las unidades académicas y administrativas.

3. Comuníquese la presente resolución al Centro de Informática y al Consejo Universitario para su publicación en La Gaceta Universitaria.

Dr. Henning Jensen Pennington
Rector

RECTORIA

Adjunto: Lo indicado

75 ANIVERSARIO

Directrices de Seguridad de la Información de la Universidad de Costa Rica

CAPÍTULO 1.
INTRODUCCIÓN

ARTÍCULO 1. La Universidad de Costa Rica reconoce que la información desempeña una función cada vez más importante en todos los aspectos del quehacer de la Comunidad Universitaria y se constituye en un componente indispensable para llevar a cabo los procesos institucionales que permiten el logro de los objetivos de la Universidad.

ARTÍCULO 2. La Universidad de Costa Rica conoce también que la información es un activo que tiene igual relevancia que los recursos tradicionalmente importantes como la infraestructura, equipos y recursos financieros y por consiguiente, debe ser debidamente protegida.

ARTÍCULO 3. Consecuentemente, la Institución se ha dado a la tarea de adoptar un conjunto de Directrices técnicas de Seguridad de Información, que además de tener como premisa básica la protección de la información perteneciente a la Universidad y/o en su custodia, constituye el fundamento de la cultura que en materia de seguridad de la información desea establecer, reforzar, implementar e incorporar en su diario quehacer, con miras no sólo a lograr un manejo eficiente de sus recursos informáticos, acorde con el interés público y en estricta concordancia con el ordenamiento jurídico costarricense, sino por sobre todo, a propiciar la eficiencia en las labores y el mejoramiento constante de los servicios que le dan fundamento a la Institución.

ARTÍCULO 4. Estas Directrices técnicas de seguridad de información institucionales tienen como objetivos básicos:

a) Proveer una guía general con respecto a las conductas que se esperan de la Comunidad Universitaria y grupos de interés de la Universidad en materia de seguridad de la información.
b) Resaltar la responsabilidad de la Comunidad Universitaria y grupos de interés de la Universidad con respecto a la protección y manejo adecuado de los recursos informáticos.
c) Informar a la Comunidad Universitaria y grupos de interés de la Universidad sobre los riesgos de seguridad de la información a los que se puede enfrentar y las medidas necesarias para mitigar y/o administrar correctamente tales riesgos.
d) Guiar a la Comunidad Universitaria y grupos de interés de la Universidad en la toma de decisiones responsables con respecto a la protección de los sistemas y recursos de información.

e) Evidenciar el papel activo de la Comunidad Universitaria y grupos de interés en la estructura de seguridad de la información de la Universidad.

f) Generar conciencia en los Jerarcas y Titulares Subordinados con respecto a la importancia de la seguridad de la información como elemento crítico a tener en cuenta en el cumplimiento de los objetivos de la Universidad y de aquellos consignados en su Plan Estratégico.

g) Guiar a los Jerarcas y Titulares Subordinados en la toma de decisiones con respecto a la protección de los sistemas de información y el establecimiento de controles adecuados a las necesidades de la Universidad.

h) Advertir a los Jerarcas y Titulares Subordinados sobre la necesidad de:

- h.1) Dar cumplimiento a los requisitos legales, reglamentarios y contractuales aplicables a la Universidad, conforme a esta normativa.
- h.2) Dar cumplimiento a los requerimientos de capacitación adecuados a las necesidades de la Universidad.
- h.3) Manejar, prevenir y detectar en su debido tiempo, instrucciones maliciosas que sean capaces de afectar los sistemas informáticos de la Universidad.
- h.4) Prever acciones para mantener en todo momento, la continuidad de los servicios críticos de la Universidad.
- h.5) Tomar acciones en caso de violación a los Directrices Técnicas de Seguridad de Información.
- h.6) Brindar una guía básica para la ejecución de auditorías de sistemas, pruebas de intrusión y análisis y valoración de riesgos.

CAPÍTULO 2.
ÁMBITO DE APLICACIÓN

ARTÍCULO 5. Estas directrices son de acatamiento obligatorio para la Comunidad Universitaria y los grupos de interés de la Universidad.

CAPÍTULO 3.
GLOSARIO DE TÉRMINOS Y DEFINICIONES

ARTÍCULO 6. Glosario de términos y definiciones:

a) **Directrices Técnicas de Seguridad de la Información de la Universidad de Costa Rica (DTSI):** compendio de normas que deberán aplicar obligatoriamente el personal Usuario (estudiantes, administrativos y docentes), usuario RIDs (Administrador de Recursos Informáticos Desconcentrados), Jerarcas y Titulares Subordinados[1] (Direcciones) y los grupos de interés de la Universidad

b) **Usuario RIDs:** Personal designado como Administrador de Recursos Informáticos

1 Ley de Control Interno

Desconcentrados, encargado de la gestión y monitoreo de la plataforma de acceso, herramientas de trabajo informáticas, sistemas de telecomunicaciones y la administración del Hardware y el Software, de cada entidad institucional (Unidad, Centro, Facultad, Escuela y afines) a la que esté asignado.

c) **Grupos de interés:** Contratistas, proveedores y demás personas ajenas a la Universidad que tengan relación con ésta.

d) **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad[2].

e) **Bases de seguridad de la información**: Contiene las bases para la comprensión de los antecedentes, objetivos, rango de operación, alcance, razones de adopción, régimen sancionatorio y demás, elementos que proporcionan el fundamento para la aplicabilidad y obligatoriedad del documento de Directrices Técnicas de Seguridad de la Información (en adelante "DTSI") de la Universidad de Costa Rica.

f) **Mecanismos criptográficos:** Algoritmos, protocolos criptográficos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

g) **Estándares de código abierto:** Lineamientos en la implementación de programas y sistemas que incrementen y permitan la compatibilidad e interoperatividad entre distintos componentes de hardware y software, ya que cualquiera con el conocimiento técnico necesario y recursos, puede construir productos que trabajen con los de otros vendedores, los cuales comparten en su diseño base el estándar.

CAPÍTULO 4.
GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 7. El gobierno de seguridad de la información en la Universidad de Costa Rica es la estructura a través de la cual se establecen los objetivos institucionales en materia de seguridad y se determinan los medios para alcanzar dichos objetivos y monitorear el desempeño. La estructura y los medios incluyen la estrategia, lineamientos, procedimientos, planes estratégicos y operativos, sensibilización y capacitación, administración de riesgos, controles y actividades de seguimiento.

CAPÍTULO 5.
DIRECTRIZ GENERAL DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 8. "La Universidad de Costa Rica garantizará la seguridad de la información ante cualquier amenaza de interrupción en la continuidad de los procesos, minimizando

2 ISO/IEC 27001

los riesgos y maximizando el retorno de las inversiones y oportunidades de crecimiento de la Institución, mediante un proceso de implementación y mantenimiento de controles de seguridad, que permitan el nivel adecuado de integridad, disponibilidad y confidencialidad de la información, con un tratamiento óptimo de riesgos y el cabal cumplimiento de los requerimientos legales, contractuales y regulatorios que le resulten aplicables en la materia.

Para su adecuada implementación contará con un Sistema de Gestión de la Seguridad de la Información, que tiene como eje fundamental el involucramiento de las personas con responsabilidad estratégica en la Universidad, quienes serán las encargadas de liderar el proceso de seguridad de la información y la participación del personal. Son instancias clave en este proceso, el Consejo Universitario y la Rectoría a través del compromiso en procura de los recursos necesarios para la buena marcha del Sistema de Gestión de Seguridad de la Información, la divulgación y el cumplimiento del mismo en toda la Institución".

CAPÍTULO 6.
SEGURIDAD ORGANIZACIONAL (INFRAESTRUCTURA INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN)

ARTÍCULO 9. La Infraestructura Integral de Seguridad de la Información es uno de los componentes esenciales de la Universidad, diseñado específicamente para:

a) Apoyar los objetivos integrales emitidos por el Comité Gerencial de Informática (CGI) de la Universidad, procurando la mayor eficiencia en las actividades, la menor pérdida de recursos, la toma asertiva y en tiempo de decisiones y el establecimiento de controles costo-eficientes.
b) Procurar la seguridad de las comunicaciones y proveer una adecuada protección a los recursos informáticos y de información.
c) Complementar los requerimientos legales, normativos, contractuales y estatutarios aplicables a la Universidad, en materia de seguridad de la información.

ARTÍCULO 10. La infraestructura de Seguridad de la Información se refiere tanto a la infraestructura técnica-informática, como a la normativa aprobada y exigible en la Universidad en materia de seguridad, al proceso de valoración de riesgos, a los programas de sensibilización y capacitación, que deben ser adoptados como una práctica dentro de la cultura organizacional de la Institución, al trabajo conjunto de todos los actores dentro del proceso de Seguridad de la Información, a la verificación de cumplimiento integral y por último, a la labor continuada y sinérgica de todos estos componentes.

ARTÍCULO 11. Infraestructura de Seguridad de la Información: Todas las personas que conforman la Universidad de Costa Rica, tienen la obligación ineludible de conocer y respetar las disposiciones de Seguridad de la Información establecidas por la

Universidad, las cuales se divulgarán para el conocimiento de la Comunicad Universitaria y de los grupos de interés en los medios que así se establezca.

ARTÍCULO 12. Seguridad de la Información en la definición de perfiles de trabajo y en la asignación de recursos: La seguridad de la información, deberá ser considerada como un factor fundamental en la definición y elaboración de los perfiles de puestos y en la asignación de recursos a lo interno de la Universidad, por cuanto la divulgación o acceso indebido de la misma, impactaría significativamente a la Institución.

ARTÍCULO 13. Capacitación del personal: La Universidad promoverá la capacitación adecuada y continua en materia de seguridad de la información para todos sus funcionarios y funcionarias, los cuales, obligatoriamente recibirán la capacitación que se disponga.

ARTÍCULO 14. De los procesos disciplinarios: La Universidad aplicará procesos disciplinarios en caso de incumplimiento de la normativa aplicable en materia de seguridad de la información.

CAPÍTULO 7.
CLASIFICACIÓN, CONTROL Y ASEGURAMIENTO DE BIENES DE CÓMPUTO Y COMUNICACIONES

ARTÍCULO 15. Se requiere brindar un grado apropiado de protección a los bienes de cómputo y comunicaciones de la Universidad, así como a la información perteneciente a la institución y/o en su custodia , poniendo especial énfasis en la clasificación de la información, como elemento definitorio para establecer los requerimientos de confidencialidad, integridad y disponibilidad de la misma.

ARTÍCULO 16. Responsabilidades sobre los bienes: Toda jefatura deberá asignar y controlar el uso de los bienes dentro de su oficina e implementar controles apropiados para cada uno de ellos. Toda persona usuaria que reciba y tenga bajo su custodia bienes de la institución, será responsable por ellos y por cualquier daño, pérdida o abuso, empleo ilegal que le sea imputable por falta al deber de cuidado, negligencia o dolo. Se deberá entonces rendir cuentas por todos los recursos informáticos de la Universidad de Costa Rica.

ARTÍCULO 17. Clasificación de la información: La información deberá ser clasificada para señalar la necesidad, la prioridad y el grado de protección que esta requiere y dicha clasificación deberá tomar en cuenta su valor, requerimientos legales e importancia para la Universidad. La clasificación de la información tendrá como objetivo primordial asegurar la confidencialidad, integridad y disponibilidad de la información.

La clasificación de la información, determinará el nivel al que la información debe ser controlada o asegurada y es indicativa del valor que la misma tiene como activo preferente de la Universidad.

CAPÍTULO 8.
RESGUARDO Y PROTECCIÓN DE LA INFORMACIÓN

ARTÍCULO 18. La protección de la información por parte del personal usuario, como un elemento fundamental en la cadena de aseguramiento de ésta, aborda la necesidad de considerar al recurso humano como elemento prioritario en la protección de la información, estableciendo controles referentes a la propiedad de la información, la elaboración de respaldos, y la protección de registros.

ARTÍCULO 19. Propiedad de la información: Toda la información que se almacena, transita, es recopilada, distribuida, reproducida, procesada y/o creada en los sistemas de información de la Universidad de Costa Rica, será considerada, para efectos de la gestión en seguridad de la información, como propiedad de la Universidad, salvo que el ordenamiento jurídico establezca lo contrario. Por lo tanto, no podrá bajo ninguna circunstancia, ser transmitida en manera alguna a terceros, modificada ni eliminada, sin contar con autorización formal para ello, por parte de los Jerarcas y Titulares Subordinados responsables de la Información.

ARTÍCULO 20. Confidencialidad de la información: La información propiedad de la Universidad de Costa Rica y/o en su custodia será tratada con extrema cautela y deberá ser conocida únicamente por quienes estén expresamente autorizados para tales efectos. Por consiguiente, cuando se tenga duda sobre la clasificación de la información de que se trate, la misma deberá ser considerada como información sometida a requerimientos de confidencialidad, mientras no se determine lo contrario.

ARTÍCULO 21. Respaldos y recuperación de la Información: La información que la Universidad de Costa Rica determine como esencial deberá ser respaldada y resguardada en instalaciones seguras y controladas, a fin de que la misma pueda recuperarse una vez ocurrido un desastre, siniestro, emergencia o falla en/de los dispositivos y/o sistemas. Los Jerarcas y Titulares Subordinados deberán velar porque existan procedimientos y controles en sus áreas y unidades, que permitan recuperar la información y que dichos procedimientos y controles sean periódicamente evaluados, para asegurar una continuidad de las operaciones en productos y servicios.

CAPÍTULO 9.
REPORTE Y MANEJO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 22. El manejo adecuado y responsable de los incidentes y anomalías en materia de Seguridad de la Información tiene como principal objetivo brindar la guía adecuada para administrarlos, monitorear su ocurrencia y minimizar los daños causados por éstos; tomando las medidas correctivas que sean necesarias y aprender de las experiencias. Dichos incidentes y anomalías pueden presentarse en el entendido de que toda acción errada u omisión a este respecto, tiene el potencial de intensificar o agravar consecuencias no deseadas para la Institución.

ARTÍCULO 23. Reporte de incidentes de seguridad de la información: Los incidentes que afectan la seguridad de la información propiedad de la Universidad de Costa Rica y/o en su custodia, deberán ser comunicados de manera rápida al ente encargado, en forma eficiente y controlada mediante canales oficiales debidamente aprobados, tomando siempre en consideración la imagen de seriedad y confiabilidad de la Universidad.

ARTÍCULO 24. Reporte de debilidades en materia de seguridad de la información: El personal de la Universidad de Costa Rica está en la obligación inexcusable de reportar al ente encargado, cualquier debilidad en la seguridad de la información y de conocer los mecanismos y procedimientos aprobados por la Universidad para hacer este tipo de reportes. El reporte deberá hacerse en el mismo momento en que la persona note la debilidad, a fin de que se pueda tomar acción inmediata y se proceda a instaurar los controles adecuados para corregirla.

ARTÍCULO 25. Uso exclusivo de los recursos informáticos de la Universidad: Los recursos informáticos de la Universidad de Costa Rica podrán ser utilizados únicamente para los efectos para los que fueron asignados. La Universidad no tolerará ningún otro tipo de usos, aún cuando los mismos se pretendan llevar a cabo ocasionalmente.

ARTÍCULO 26. Prohibición de causar incidentes de seguridad: Está estrictamente prohibido al Personal Usuario corromper, inutilizar, alterar, modificar y/o en forma alguna impedir el funcionamiento de los recursos informáticos de la Universidad de Costa Rica, sin contar con permiso expreso válidamente emitido para ello. También le está terminantemente prohibido al Personal Usuario hacer pruebas de vulnerabilidad a los recursos informáticos de la Universidad, sin contar con autorización expresa y formal válidamente emitida para ello.

CAPÍTULO 10.
SEGURIDAD FÍSICA

ARTÍCULO 27. Procurar un ambiente integral de Seguridad de la Información, resguardando la parte de infraestructura física como el esquema básico de aseguramiento. La administración superior de la Universidad de Costa Rica, al implementar su esquema integral de administración de seguridad de la información, proporcionará protección a todos sus elementos, como parte de un sistema; así, el objetivo de esta sección es señalar la importancia del trabajo, planeación y acción conjuntos que permita se tomen en cuenta aspectos de seguridad informática en la creación, constitución e implementación de seguridad física y viceversa.

ARTÍCULO 28. Áreas seguras y controles de acceso físico: Con el fin de impedir accesos no autorizados, daños y/o intrusiones a/en las sedes de procesamiento de datos de la Universidad de Costa Rica, las instalaciones de procesamiento de la información crítica o sensible, propiedad de la Institución y/o en su custodia, deberán estar en áreas resguardadas por un perímetro de seguridad definido, debidamente provisto para regular el acceso a fin de que sólo el personal autorizado pueda ingresar.

ARTÍCULO 29. Seguridad de los bienes físicos: Con el objetivo primordial de evitar que se den daños y/o exposiciones al riesgo de los bienes institucionales, así como la interrupción de las actividades críticas de la Universidad de Costa Rica, cada persona que tenga un equipo de cómputo asignado, está en la obligación de conocer y cumplir el "REGLAMENTO PARA LA ADMINISTRACIÓN Y CONTROL DE LOS BIENES INSTITUCIONALES DE LA UNIVERSIDAD DE COSTA RICA". Asimismo, está estrictamente prohibido fumar, comer o beber cerca de los recursos informáticos de la Universidad y en aquellas áreas que hayan sido delimitadas con tal prohibición.

ARTÍCULO 30. Seguridad de bienes físicos fuera de la Organización: Los recursos informáticos de la Universidad de Costa Rica, podrán ser utilizados fuera de la institución únicamente con autorización previa válidamente emitida por la autoridad correspondiente. El Personal Usuario deberá observar en todo momento las disposiciones establecidas para la debida protección de estos bienes dentro y fuera de las instalaciones de la Universidad.

ARTÍCULO 31. Controles generales contra la exposición al riesgo de robo y/o hurto de la información: Todo el personal Usuario de la Universidad de Costa Rica, velará inexcusablemente para que toda la información confidencial, así como los bienes institucionales valiosos que le han sido asignados, estén adecuadamente protegidos en todo momento. Esta disposición incluye no dejar expuesta en su escritorio, pantalla, impresoras y equipos de fax, información confidencial o sensible, propiedad de la

Institución y/o en su custodia. Asimismo, a la estricta observancia de todos las Directrices de seguridad de información establecidas en las DTSI.

CAPÍTULO 11.
GESTIÓN DE LA SEGURIDAD DE LAS OPERACIONES

ARTÍCULO 32. La seguridad de la información debe ser considerada como parte fundamental en los procesos operacionales institucionales, a fin de proteger y garantizar tanto el cumplimiento de los objetivos propios de la Universidad de Costa Rica, como de los deberes que le impone el ordenamiento jurídico, el bloque de legalidad y demás compromisos contractuales formalmente adquiridos.

ARTÍCULO 33. Responsabilidades y procedimientos: Los procedimientos operacionales de la Universidad de Costa Rica deberán ser planeados, creados, aprobados y documentados, con base en los requerimientos específicos de cada proceso. Deberá tomarse en consideración el abordaje de aspectos tales como: control satisfactorio de cambios en las operaciones, segregación de funciones, separación de ambientes de desarrollo y producción, requisitos para la contratación de personas ajenas a la Institución para la administración de ambientes de procesamiento de información y cualquier otro indicado en las DTSI.

ARTÍCULO 34. Planificación de la capacidad y aprobación de los sistemas: Se deberán definir y documentar los criterios de capacidad de cada uno de los sistemas a implementar en la Universidad de Costa Rica, así como criterios de aprobación para nuevos sistemas de información, actualizaciones, modificaciones y nuevas versiones, incluyendo procedimientos de prueba, sugeridos por el Comité Gerencial de Tecnologías de Información. Será requisito ineludible para la aprobación de todo sistema, de sus modificaciones o actualizaciones y de su paso al ambiente de producción, el que se compruebe que los mismos cumplan y hayan cumplido durante todo su proceso de desarrollo y pruebas, con los requerimientos de seguridad de la información aprobados por la Universidad.

ARTÍCULO 35. Controles contra instrucciones maliciosas: La Universidad de Costa Rica proveerá para todos sus equipos que así lo requieran, un software antivirus que le proteja contra instrucciones maliciosas. Será responsabilidad del Personal Usuario al cual se le asigna el equipo, velar por que la aplicación antivirus esté instalada y funcionando en su última versión , asimismo, reportar cualquier irregularidad que detecte al respecto. El uso de cualquier tipo de software en los equipos de la Institución debe necesariamente contar con la aprobación de las autoridades competentes.

ARTÍCULO 36. Administración de la red: La Universidad de Costa Rica confiará la administración de sus redes únicamente a personal que se encuentre debidamente

calificado y será responsabilidad del Centro de Informática velar porque dicho personal se capacite adecuada y regularmente. La administración de las redes de la Institución deberá contemplar los factores de protección necesarios para garantizar que a cada persona se le asigne acceso a los servicios que estrictamente necesite en virtud de su relación para con la Universidad, asimismo, abordará aspectos de seguridad de la información para el acceso remoto a los servicios de red, monitoreo, auditoría y en general todo lo establecido en las DTSI.

ARTÍCULO 37. Eliminación de medios de almacenamiento: La eliminación de medios informáticos de almacenamiento, sólo será llevada a cabo por el personal autorizado de la Unidad de Bienes Institucionales; previa eliminación de la información confidencial, crítica, sensible o de uso interno de la Universidad contenida en éstos y debe ser llevada a cabo por la unidad responsable de dicha información, en estricto cumplimiento con los procedimientos aprobados por la Universidad de Costa Rica para tales efectos. No se encomendará a personas ajenas a la Institución la destrucción de medios informáticos de almacenamiento, sin autorización escrita válidamente emitida por quien tenga autoridad para ello.

ARTÍCULO 38. Mantenimiento de recursos informáticos: Quienes hayan sido designados a tales efectos, deberán implementar estrictamente los controles y procedimientos establecidos en las DTSI, para brindar un adecuado mantenimiento a los recursos informáticos de la Institución con el objetivo de mantener la integridad, disponibilidad y confiabilidad de los servicios de procesamiento de información. Estas actividades incluyen pero no se limitan a: labores de respaldo y recuperación de la información, bitácoras de actividades de mantenimientos o registro de fallas, entre otros.

CAPÍTULO 12.
GESTIÓN DE LA SEGURIDAD EN LAS COMUNICACIONES

ARTÍCULO 39. La gestión y administración de la seguridad en las comunicaciones consiste fundamentalmente en prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad de la información, que pudiesen generarse en la transmisión e intercambio de la misma con el objetivo de mantener la integridad, disponibilidad y confiabilidad de los servicios de procesamiento de información.

ARTÍCULO 40. Intercambios de información y software: La Universidad de Costa Rica procurará la protección de la información de su propiedad y/o en su custodia y del software adquirido, instalado y utilizado, en el intercambio de éstos con terceras personas u organizaciones y a la vez, velará porque tales intercambios se lleven a cabo dentro de un ámbito de absoluta legalidad.

ARTÍCULO 41. Uso aceptable de las telecomunicaciones: Los medios, servicios y canales de telecomunicación (de cualquier naturaleza) provistos por la Universidad, incluyendo, pero sin limitarse a: teléfonos de nueva generación, radios, computadores, mecanismos de teleconferencia y videoconferencia, mensajería electrónica, entre otros, lo son únicamente para efectos relacionados con la actividad de la persona usuaria para con la Universidad de Costa Rica. Dichos medios, canales y/o servicios se proveen para la comunicación de información de interés para la Universidad, nunca para fines ilegales y/o no autorizados formalmente. Toda persona usuaria de este tipo de recursos provistos por la Universidad, deberá utilizarlos en estricto apego a las Directrices establecidas para ese fin en las DTSI.

ARTÍCULO 42. Uso aceptable de internet: El personal usuario deberá tener presente que el uso de internet es un privilegio temporal concedido por la Universidad de Costa Rica, permitido para efectos labores permitidas de docencia, investigación, acción social, trámites administrativos, trámites en línea gubernamentales, entre otros. De esta manera, si la Universidad considera que el servicio está siendo objeto de abuso, podrá retirarlo, eliminarlo, restringirlo o suspenderlo, sin derivar por ello responsabilidad alguna, ya que corresponde a la Institución ejercer mecanismos de control interno y a la vez, velar por el interés público propiciando el mejor uso de los recursos a su cargo. El uso de éste servicio deberá realizarse en estricto apego a las DTSI.

ARTÍCULO 43. Uso aceptable del correo electrónico: La Universidad de Costa Rica dispondrá de un servicio de correo electrónico únicamente para ser utilizado en actividades que sean de su interés. Por lo tanto, su uso estará regido por las condiciones que establezca la Universidad dentro los límites permitidos por el ordenamiento jurídico costarricense, sin incurrir por ello en responsabilidad alguna. Toda persona usuaria de este servicio estará en la obligación de hacer uso del mismo en estricto apego a las Directrices establecidas por la Institución en las DTSI.

CAPÍTULO 13.
CONTROL DE ACCESOS

ARTÍCULO 44. Se establecen los controles para el acceso a la información, a los sistemas y a los procesos institucionales, mismos, que deberán ser consistentes con los requerimientos de seguridad propios de la información de que se trate y de los objetivos que se haya trazado la Universidad, contemplados en las DTSI , así como en los estándares, lineamientos y procedimientos formalmente aprobados.

ARTÍCULO 45. Requerimientos corporativos del control de accesos: La Universidad de Costa Rica controlará el acceso a la información, a los servicios, sistemas y a los

procesos institucionales de acuerdo a las Directrices que para ese fin se establecen, así como, en los estándares y procedimientos formalmente aprobados.

ARTÍCULO 46. Administración de acceso de usuarios: La Universidad de Costa Rica establecerá procedimientos formales para la asignación de derechos de acceso, para el registro y eliminación de usuarios, administración de privilegios (permisos), así como, para la revisión periódica de los derechos de acceso de los usuarios.

ARTÍCULO 47. Responsabilidad en el uso de contraseñas: Toda persona usuaria de sistemas de información de la Universidad de Costa Rica contará con al menos una contraseña, que se validará antes del acceso a los sistemas y será de su exclusiva responsabilidad actuar de acuerdo a lo establecido.

ARTÍCULO 48. Consecuencias del mal uso de las contraseñas: Las contraseñas de acceso son responsabilidad de la persona usuaria a quien le fueron asignadas, por lo que cualquier consecuencia adversa que derive de su mal uso, generado por descuido, negligencia o dolo, deberá ser asumida directamente por dicha persona. Sin perjuicio de lo anterior, cualquier violación u omisión a lo aquí estipulado será considerada importante y la Universidad de Costa Rica tomará las medidas administrativas, laborales, civiles y/o penales que la ley le permita, para sancionar a los responsables.

CAPÍTULO 14.
CONTRATISTAS, PROVEEDORES Y DEMÁS PERSONAS AJENAS A LA UNIVERSIDAD

ARTÍCULO 49. La interacción de personas ajenas a la Universidad de Costa Rica, será objeto de regulación en materia de seguridad de la información. Se considerará a los terceros que interactúan con la Universidad dentro del esquema de seguridad de la información, de manera que se provea una guía general sobre los requerimientos básicos que éstos deberán cumplir y sobre los controles adecuados que se deberán instaurar, para administrar correctamente su participación.

ARTÍCULO 50. Seguridad de la información frente al acceso por parte de terceros: La Universidad de Costa Rica permitirá el acceso físico y/o lógico a personas ajenas a la Universidad únicamente, cuando de previo se haya demostrado la necesidad justificada y de conveniencia para la Institución de brindar dicho acceso.

ARTÍCULO 51. Control de accesos para terceras partes: Todos los accesos físicos y lógicos de personas ajenas a la Universidad de Costa Rica deberán estar sometidos a controles y parámetros de autorización y autenticación que permitan salvaguardar la integridad, disponibilidad y confidencialidad de los recursos informáticos y de información de la Institución.

ARTÍCULO 52. Requerimientos de seguridad en contratos con contratistas:
La Universidad de Costa Rica verificará los antecedentes a los contratistas para determinar la idoneidad de los mismos en los servicios y labores a contratar. Una vez verificada la idoneidad del contratista, se suscribirán contratos formales entre las partes que contengan todos los requerimientos y disposiciones en materia de seguridad de la información que los contratistas deben resguardar. Solo se otorgará acceso apropiado de la información y de las instalaciones a los contratistas, luego de la implementación de controles apropiados y la aceptación y firma de documentos legales que definan las condiciones de conexión y acceso otorgado.

CAPÍTULO 15.
DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

ARTÍCULO 53. Los procesos de desarrollo y mantenimiento de sistemas de información, deben asegurar que se tomen en cuenta los requerimientos de seguridad de la información, debidamente aprobados por la Institución.

ARTÍCULO 54. Requerimientos de seguridad en los sistemas: La Universidad de Costa Rica promoverá que la seguridad de la información sea un elemento intrínsecamente incorporado a los sistemas de información, tanto en su infraestructura, como en su diseño e implementación.

ARTÍCULO 55. Seguridad en los sistemas de aplicación: Deberán crearse controles para prevenir las pérdidas, modificaciones y/o el uso no autorizado de los datos contenidos en los sistemas de aplicación de la Universidad de Costa Rica. Los controles a implementar incluyen validación de datos de entrada, verificación de datos generados, autenticación de mensajes, validación de datos de salida y cualesquier otros controles establecidos en las DTSI , así como en sus procedimientos asociados.

ARTÍCULO 56. Controles criptográficos: La Universidad de Costa Rica procurará la implementación de técnicas y mecanismos criptográficos estandarizados en toda la Institución que coadyuven en la protección de la confidencialidad, autenticidad e integridad de la información sensible. Se instaurarán normas y procedimientos que como mínimo regulen elementos como: controles criptográficos, administración de claves y llaves criptográficas, encripción o cifrado, firma digital y no repudio.

ARTÍCULO 57. Seguridad de los archivos y de los procesos de desarrollo y soporte: La Universidad de Costa Rica promoverá la implementación de controles que permitan garantizar que los proyectos y actividades de soporte de tecnología de la información se lleven a cabo de manera segura, manteniendo la seguridad del software y de la

información de los sistemas de aplicación. Estos controles incluyen, pero no se limitan a: software en producción, protección de los datos resultado de pruebas aplicadas a los sistemas, protección de la información utilizada en los procesos de prueba; acceso al código fuente, control de cambios, desarrollo externo de software. El Centro de Informática controlará el cumplimiento de esta directriz.

CAPÍTULO 16.
ADQUISICIÓN, USO ACEPTABLE Y RESGUARDO DE LOS EQUIPOS INFORMÁTICOS

ARTÍCULO 58. En la utilización de los equipos informáticos el tema de la seguridad de la información debe ser uno de los elementos fundamentales a considerar. En este aparte, se aborda la necesidad de que en la adquisición, uso y resguardo de equipos informáticos y hardware de la Universidad de Costa Rica, se consideren aspectos de seguridad de la información.

ARTÍCULO 59. Adquisición del hardware: La Universidad de Costa Rica de previo a proceder a la adquisición de equipo informático institucional, evaluará y analizará los requerimientos de seguridad de la información que transita o se encuentra en los sistemas de la Institución, en los que se utilizará el equipo a adquirir, para lo cual, el Centro de Informática creará y documentará procedimientos de análisis claros que guíen la selección y adquisición del hardware.

ARTÍCULO 60. Protección del hardware: El equipo provisto por la Universidad de Costa Rica será considerado en todo momento propiedad de la Institución y por lo tanto, su uso y resguardo deberá realizarse en todo momento y en estricto apego a lo dispuesto en las DTSI , incluyendo, pero sin limitarse a las Directrices para el uso del equipo dentro y fuera de las instalaciones de la Universidad y uso de equipo ajeno en la red y/o sistemas de la Institución.

CAPÍTULO 17.
ADQUISICIÓN, USO ACEPTABLE Y RESGUARDO DE LA INFORMACIÓN

ARTÍCULO 61. Se debe resguardar la seguridad en la información propiedad de la Universidad y/o en su custodia, al adquirir, instalar y utilizar software, procurando el uso efectivo de este, independientemente del tipo de licenciamiento o tipo de distribución ("Freeware", "Shareware", "Adware" y Software Libre), que garantice que los formatos utilizados en el resguardo de la información cumplan con los estándares de código abierto. Así mismo, se pretende proteger a la organización de adquirir, instalar y utilizar

software ilegal y/o inadecuado a las necesidades de la Universidad de Costa Rica.

ARTÍCULO 62. Adquisición, instalación y uso del software: La Universidad de Costa Rica procurará que sus procesos de adquisición, instalación y uso de software, contemplen en toda ocasión prácticas dirigidas al resguardo de la información propiedad de la Institución y en su custodia, para lo cual, impulsará mediante el Centro de Informática Directrices generales que guíen los procesos de adquisición de software institucional, incluyendo Directrices a tomar en cuenta en la elaboración de carteles y contratos, así como, en el software hecho a la medida para la Universidad y pruebas generales en cualquier software a adquirir.

ARTÍCULO 63. Protección del software: La Universidad de Costa Rica regulará el uso de software institucional en estricto apego a las DTSI, y velando por el respeto a derechos de propiedad intelectual, de autoría y demás derechos conexos existentes sobre el software de que se trate, así como, a los términos y restricciones de las licencias respectivas. Asimismo, sólo autorizará el uso del software institucional a quienes así lo requieran, con base en una necesidad comprobada en virtud de su relación para con la Universidad.

CAPÍTULO 18.
ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS OPERACIONES

ARTÍCULO 64. Contrarrestar las interrupciones a las actividades institucionales y proteger los procesos críticos de la Universidad de los efectos de fallas significativas o desastres.

ARTÍCULO 65. Continuidad de las operaciones: La Universidad de Costa Rica impulsará todas las previsiones necesarias para garantizar la continuidad de las operaciones institucionales, a fin de que sus procesos críticos se mantengan en pie y los objetivos que le dan su razón de ser, se cumplan adecuadamente.

ARTÍCULO 66. Planes de continuidad: La Universidad de Costa Rica desarrollará planes para contrarrestar las interrupciones de sus actividades y para proteger procesos críticos de los efectos de fallas significativas o desastres.

ARTÍCULO 67. Ejecución de los planes de continuidad: Los planes de continuidad de la Universidad de Costa Rica deberán ser elaborados e implementados para mantener o restablecer la operación de la Universidad y asegurar la disponibilidad de la información en plazos mínimos, una vez ocurrida una emergencia, evento de falla y/o interrupción de servicios, que afecte los procesos críticos.

CAPÍTULO 19.
CONTROL DE CUMPIMIENTO

ARTÍCULO 68. Para vigilar el debido cumplimiento de las responsabilidades asignadas en materia de seguridad de la información, la Universidad de Costa Rica implementará mecanismos pertinentes que permitan verificar el cumplimiento de la normativa aplicable.

ARTÍCULO 69. La Universidad de Costa Rica procurará:

a) Cumplimiento de normativa vigente: Evitar infracciones y violaciones al orden jurídico establecido, a la normativa interna de la Universidad de Costa Rica y a las obligaciones contractuales a las cuales ésta está sujeta. Por lo tanto, cada persona usuaria tiene la responsabilidad de desarrollar su relación con la Institución en estricto acato a la legislación aplicable, a la buena fe y a las buenas costumbres. Quien violentando lo estipulado en las DTSI , actúe de manera ilegal, de mala fe y/o en irrespeto a las buenas costumbres, responderá personalmente por cualquier consecuencia adversa que de su comportamiento derive.

b) Verificación de cumplimiento: Implementar un control adecuado de cumplimiento, que verifique no solamente la participación de los diferentes grupos de usuarios, sino también, el seguimiento de las disposiciones normativas, reglamentarias y/o contractuales en materia de seguridad de la información.

CAPÍTULO 19.
DOCUMENTOS LEGALES A LAS DIRECTRICES TÉCNICAS

ARTÍCULO 70. Se establece la necesidad de contar con una plataforma legal vinculante, que le permita a la Universidad contar con documentos (legales) de apoyo, que faciliten el cumplimiento y seguimiento de la normativa adoptada en materia de seguridad de la información.

ARTÍCULO 71. Documentos legales de apoyo a la gestión de seguridad de la Información: Se dotará de una plataforma legal de apoyo vinculante, que le permitirá a la Institución contar con las herramientas necesarias, a fin de hacer efectivas las estipulaciones contenidas en dichas normas. Esta plataforma les brindará a la vez a los usuarios de los recursos informáticos de la Universidad de Costa Rica, un referente básico de sus principales obligaciones y comportamientos esperados.

ARTÍCULO 72. Suscripción de documentos: Requerirá del personal usuario, la suscripción de documentos que le expongan su responsabilidad la materia de Seguridad de la Información y se indiquen las potestades de monitoreo legítimo y necesario, que

habrá de llevar a cabo la Universidad de Costa Rica con respecto a sus recursos informáticos. En pleno cumplimiento con la normativa aplicable se requiere de la suscripción de por lo menos los siguientes documentos:

a) Acuerdo de confidencialidad
b) Recibo de número de cuenta de usuario
c) Conocimiento de las Directrices Técnicas de Seguridad de la Información de la Universidad de Costa Rica
d) Adjudicación de responsabilidad por el manejo del software
e) Aceptación de revisión, respaldo de información y monitoreo de los recursos informáticos
f) Correo electrónico.