REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA NACIONAL

(Aprobado mediante Acuerdo 11-15-2022, tomado por el Consejo Universitario en la Sesión Ordinaria No. 15-2022, celebrada el jueves 14 de julio del año 2022, a las nueve horas, según el Artículo 20 del Capítulo XI. Comisión Interna de Reglamentos. Publicado en el diario oficial La Gaceta No. 152 del 11 de agosto del año 2022, sección de Reglamentos).

CAPÍTULO I
GENERALIDADES

Artículo 1. Ámbito de aplicación. Este reglamento regula la gestión de los dispositivos y medios informáticos dispuestos por la Universidad Técnica Nacional para el cumplimiento de sus objetivos.

Las disposiciones contenidas en este reglamento son de acatamiento obligatorio por la comunidad universitaria y personas que tengan acceso a los recursos de tecnologías de la información, en concordancia con lo establecido en el Reglamento del Sistema Universitario de Gestión Documental.

Artículo 2. Glosario de términos.

a. Contraseñas críticas: se refiere a las cuentas que se utilizan en diversos ambientes de procesamiento, con las cuales es posible efectuar actividades especializadas como la instalación de plataformas o sistemas, habilitación de servicios, actualización de software y configuración de componentes informáticos, entre otras, normalmente, tienen un mayor nivel de complejidad que las habituales.

b. Criticidad informática: se refiere a cualquier recurso informático que, en caso de fallo, cause la interrupción de al menos un servicio esencial para la Universidad.

c. Incidente de seguridad de la información: se refiere a un intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; una interrupción de los sistemas o recursos informáticos o una violación a las políticas y normas de seguridad de la información.

d. Información sensible: se refiere a la información relativa al fuero íntimo de la persona, por ejemplo, los que revelan origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

e. Necesidad de saber o menor privilegio: se refiere al principio de seguridad aplicado a las Tecnologías de la Información y la Comunicación, que consiste en otorgar, únicamente, los permisos necesarios para el desempeño seguro y eficiente de una actividad.

f. Política de seguridad: se refiere al conglomerado de normas y directrices que garantizan la confidencialidad, integridad y disponibilidad de la información, en busca de minimizar los riesgos que le afecten.

g. Procedimiento de operación: se refiere al documento que regula la actuación de la población de las personas funcionarias, en torno a un proceso técnico y administrativo.

h. Proceso: se refiere al conjunto de pasos preestablecidos para el cumplimiento de una meta específica.

i. Seguridad de la información: se refiere al conjunto de medidas reactivas y preventivas que buscan proteger la confidencialidad, integridad y disponibilidad de la información y sistemas informáticos sensibles de la Universidad.

j. Servicio tercerizado: se refiere a la contratación específica de un servicio ubicado fuera de las instalaciones universitarias o de un servicio cuyo resultado se entrega en la institución.

k. Sistemas en producción: se refiere a los servicios o sistemas informáticos dispuestos para el uso cotidiano de la población usuaria universitaria.

l. Software autorizado: se refiere al software adquirido por compra o donación mediante gestión de la Dirección de Control de Bienes e Inventarios o cualquier otro medio, que la organización dispone para el uso de la población universitaria, con la aprobación de la Dirección de Gestión de Tecnologías de la Información.

m.Transacción electrónica: se refiere a cualquier transmisión bidireccional de datos entre la Universidad y un ente externo, que amerite el cuidado y manejo adecuado de la información transmitida.

n. Usuario (a) final: se refiere a la población universitaria que utiliza los servicios tecnológicos puestos a su disposición, por la Dirección de Gestión de Tecnologías de la Información.

o. Usuario (a) funcional: se refiere a la persona usuaria que utiliza en forma práctica, operativa y única, una funcionalidad específica en alguna aplicación tecnológica universitaria.

CAPÍTULO II
ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Artículo 3. Órgano responsable. La seguridad es responsabilidad de todos, por ende, es deber de los órganos asumir compromisos alineados a la integridad, disponibilidad y confidencialidad de la información.

De acuerdo con este punto, la Universidad asegura que todas las actividades relacionadas con la seguridad de la información tengan una persona asignada que comprenda su rol y responsabilidad.

a. Administrador (a) de la seguridad de la información: es la persona asignada a la Unidad de Seguridad del Área de Gestión Estratégica. Es el responsable por el seguimiento de estándares, políticas y normas de seguridad, dentro del ámbito de la seguridad de la información institucional.

b. Área de gestión estratégica: es la responsable de la gestión, el control y seguimiento de los procesos administrativos de la Dirección de Gestión de Tecnologías de la Información, para lo cual, cuenta con ámbitos de especialización claves en el proceso informático, tales como planeación, seguridad, calidad y aprovisionamiento.

c. Comité de seguridad de la información: es el órgano técnico asesor de la Dirección de Gestión de Tecnologías de la Información en materia de seguridad de la información. Revisa y aprueba los cambios a la Política de Seguridad de la Información, además, traslada dichas modificaciones a la Dirección de Gestión de Tecnologías de la Información para que surtan efecto.

d. Consejo Universitario: es el órgano jerárquico de máximo nivel, responsable de la aprobación de la Política de Seguridad de la Información de la Universidad.

e. Contacto de seguridad de la información: es la persona designada para actuar como enlace, en materia de seguridad de la información, entre la Universidad Técnica Nacional y los terceros contratados. Su información está descrita en los contratos de referencia.

f. Contacto del servicio: es la persona, en quien el responsable del activo de la información, delega las tareas de rutina diarias sobre los activos a su cargo.

g. Custodio (a) de la Información: es la persona designada por el responsable del activo de la información para las tareas y rutinas diarias de la información a su cargo, en consecuencia, de la normativa existente. En términos generales, tiene que asegurar el inventario, la clasificación y protección, así como la definición adecuada de restricciones y clasificaciones de acceso. Es el contacto del servicio ante las personas usuarias.

h. Dirección de Gestión de Tecnologías de la Información (DGTI: corresponde a la Dirección de Gestión de Tecnologías de la Información, adscrita a la Rectoría, gestionar la dirección estratégica del área, además, de la comunicación con otras entidades para el fortalecimiento y cumplimiento de los objetivos estratégicos, procurando el manejo de la información en forma integral.

i. Director de la Dirección de Gestión de Tecnologías de la Información: es el máximo órgano administrativo y técnico que le corresponde el establecimiento y manutención de suficientes medidas preventivas de detección y corrección, las cuales aseguren, en forma razonable, que la información sea contenida y procesada a través de medios tecnológicos, garantizando la confidencialidad, integridad y disponibilidad de la información.

j. Equipo de atención: es un grupo de personas profesionales en tecnologías de la información, que reciben informes sobre incidentes de seguridad y, en consecuencia, tienen el deber de analizar y responder ante cualquier tipo de situación que ponga en riesgo la seguridad de la información.

k. Equipo de soporte técnico: es un grupo de personas con habilidades y conocimiento técnico, cuya función se centra en asistir a la población universitaria ante cualquier problema de índole tecnológico, que no requiere la manipulación de servicios o equipos críticos.

l. Rectoría: es el órgano jerárquico de mayor nivel administrativo, a quien le corresponde proporcionar las herramientas para la gestión de la seguridad de la información en la Universidad.

m.Responsable del activo de información: es garante de la adecuada gestión de los activos a lo largo de todo su ciclo de vida, puede delegar las tareas rutinarias diarias, más no la responsabilidad.

n. Responsable de la información: persona que dispone de la información, tiene la autoridad para especificar y exigir las medidas de seguridad necesarias para el cumplimiento de sus responsabilidades, pudiendo delegar los aspectos operacionales en responsables de seguridad, no así su rol de propiedad, que no puede delegarse en un tercero.

o. Seguridad de TI: es la unidad cuya función principal es dedicarse a la administración de la seguridad de la información institucional.

p. Unidad de Seguridad: es el órgano asesor de la Dirección de Gestión de Tecnologías de la Información, en el tema normativo y procedimental de seguridad de la información, adscrita al Área de Gestión Estratégica.

i. Le corresponde el establecimiento y mantenimiento de la política, los estándares, los lineamientos y los procedimientos institucionales asociados.

ii. Es de su competencia y responsabilidad mantener la vigencia de este documento mediante la actualización permanente.

iii. Es su deber el promover un proceso continuo de revisión y mejoramiento de la política, con el propósito de dotar a la Universidad de una herramienta que garantice niveles de seguridad apropiados para la gestión de las Tecnologías de la Información y la Comunicación.

iv. Es la unidad facultada para hacer las recomendaciones que estime pertinentes, para que se realicen periódicamente los ajustes necesarios a los procedimientos de operación, según corresponda, en apego a las mejores prácticas de seguridad.

Artículo 4. Cumplimiento de la seguridad. Todas las personas que, por la naturaleza de su relación con la Universidad, tengan acceso a los recursos de tecnologías de la información, deben procurar el cumplimiento de la política de seguridad y normativa, así como garantizar por todos los medios disponibles la aplicación de los procedimientos de seguridad establecidos en este reglamento.

CAPÍTULO III
GESTIÓN DE LA INFORMACIÓN

Artículo 5. Coordinación de la seguridad de la información. La Unidad de Seguridad y las personas encargadas de las diferentes unidades administrativas de la Universidad o los contactos de seguridad

de estas, son los encargados de coordinar las actividades de seguridad de la información.

Artículo 6. Incumplimiento de la política de seguridad de la información. La Unidad de Seguridad de la Dirección de Gestión de Tecnologías de la Información es la encargada de dar seguimiento a las transgresiones que se detecten a las políticas de seguridad, y comunica a la Dirección y al Jerarca correspondiente sobre los hallazgos, de manera que se tomen las medidas correctivas.

Artículo 7. Compromiso de confidencialidad. Los requerimientos de confidencialidad en servicios y productos de Tecnologías de la Información, adquiridos por la Universidad, son regulados, identificados y revisados por la Dirección de Gestión de Tecnologías de la Información, en colaboración con la Dirección General de Asuntos Jurídicos y la Dirección de Proveeduría Institucional, en periodos no mayores a un año.

Artículo 8. Uso y acceso de la información. Es deber de la Dirección General de Administración Universitaria y la Dirección de Gestión de Tecnologías de la Información, garantizar el acceso oportuno, transparente y confiable a los datos y la información institucional, en el momento en que sean requeridos y alineados al uso con los fines destinados, en concordancia con la normativa institucional.

Artículo 9. Uso de la política de seguridad y sus procedimientos. Toda documentación relacionada con la seguridad de la información de la Dirección de Gestión de Tecnologías de la Información, es de acatamiento obligatorio y de uso interno, a menos que expresamente sea creada para procesos externos.

Artículo 10. Uso responsable de datos y software autorizado. Toda persona que por la naturaleza de su relación con la Universidad, tenga acceso a los recursos de tecnologías de la información, es responsable de la información a su cargo, por lo que debe dar el debido uso a los datos y usar el software autorizado por la administración, fortaleciendo la protección de la confidencialidad, integridad y disponibilidad de la información, manejada por los sistemas computacionales y de comunicaciones de la Universidad.

En el caso de no acatar estas disposiciones, puede incurrir en responsabilidad administrativa, sin perjuicio de la responsabilidad penal o civil que pueda derivar de la falta.

Artículo 11. Excepciones a la política. Únicamente, pueden existir excepciones a la utilización de la Política de Seguridad de la Información,

en caso de fuerza mayor o un estado de necesidad, analizando las implicaciones del incumplimiento. Además, la persona responsable de la información debe presentar un formulario de aceptación de riesgos, que debe ser aprobado por la Dirección de Gestión de Tecnologías de la Información. Todo procedimiento, política o estándar, que contemple la seguridad de la información debe incluir el manejo de excepciones.

Artículo 12. Gestión del riesgo de seguridad de la información. La Dirección de Gestión de Tecnologías de la Información, en colaboración con la Unidad de Seguridad y las áreas involucradas, elabora las directrices sobre manejo, custodia y acceso de información; además, crea y revisa periódicamente un plan de gestión del riesgo. Todo lo anterior, alineado a lo establecido por el Área de Control Interno de la Dirección de Planificación Universitaria.

Artículo 13. Identificación del custodio de la información. Es deber del responsable de la unidad ejecutora, asignar a cada tipo de información una persona como responsable, quien protege en forma apropiada la información, manteniendo el control de acceso, la sensibilidad y las instrucciones de criticidad de los datos.

Artículo 14. Clasificación de la información. Es deber de la persona responsable de la información, clasificarla y protegerla, de acuerdo con la sensibilidad, el valor, la criticidad, la confidencialidad, la integridad y la disponibilidad que tenga para la Universidad**.**

Artículo 15. Categoría y perfiles de acceso. La persona, que resguarda la información, es también responsable de los datos que genera su unidad, esto en relación con las categorías de personas y perfiles de acceso a quienes se les brinda permiso para que accedan a la información o a sus partes.

Artículo 16. Identificación de la persona responsable de cada tipo de información. Es deber de la Unidad de Seguridad, mantener un inventario actualizado de las personas responsables de la información. Si la propiedad de un tipo específico de información residente en un sistema multiusuario no ha sido claramente definida o asignada a una persona administradora específica, es el Director de la Dirección de Gestión de Tecnologías de la Información, quien realiza las acciones pertinentes para que se asigne la propiedad a quien corresponda.

CAPÍTULO IV
FORTALECIMIENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Artículo 17. Compromiso con la política. Es deber de toda persona, que por la naturaleza de su relación con la Universidad, comprometerse al cumplimiento de políticas y normativa en tema de seguridad de la información, así como los procedimientos, controles, estándares de seguridad y las condiciones requeridas de confidencialidad.

Artículo 18. Enlace de seguridad de terceros. Es deber del proveedor de consultoría, que suministre bienes o servicios de tecnologías de información a la Universidad Técnica Nacional, designar al menos una persona contacto de seguridad de la información, que sirva de enlace con la Universidad para tratar los asuntos relacionados con los bienes o servicios contratados, así como con las políticas, procedimientos y estándares de seguridad vigentes.

Artículo 19. Actualización de los derechos de acceso. Todo cambio de estatus de las personas usuarias en los sistemas de la Universidad Técnica Nacional incluyendo a usuarios externos, consultores, contratistas u otros, es deber de la jefatura inmediata reportar a las personas administradoras de sistemas de información involucrados. En el caso de las personas usuarias internas, esta responsabilidad recae en la jefatura inmediata y en el de las personas usuarias externas (instituciones, empresas) es el contacto de seguridad o contraparte designado por la empresa o institución que corresponda. Los derechos de acceso a la información, por parte de la población de empleados, consultores y terceros, son eliminados en cuanto concluya la relación laboral, contrato o acuerdo.

Artículo 20. Cambios a la política de seguridad de la información. Los cambios a la política de seguridad de la información, realizados por la Unidad de Seguridad en colaboración con las áreas interesadas; es deber de la Dirección de Gestión de Tecnologías de la Información informar a los usuarios tanto internos como externos, mediante los medios de comunicación adecuados.

CAPÍTULO V
SEGURIDAD FÍSICA Y AMBIENTAL

Artículo 21. Protección del equipo informático. Para prevenir la pérdida, daño o compromiso del equipo, lo cual puede interrumpir las actividades de la Universidad, so pena de incurrir en responsabilidad administrativa y sin perjuicio de la responsabilidad penal o civil que pueda derivar de la omisión de las responsabilidades de la población universitaria; todo equipo informático, así como la información contenida en éste, deber ser protegida en forma apropiada por la persona responsable del activo.

Artículo 22. Mantenimiento al equipo informático. Es deber, únicamente de las personas autorizadas por la Dirección de Gestión de Tecnologías de la Información, llevar a cabo los servicios de mantenimiento correctivo y preventivo, al equipo informático propiedad de la Universidad Técnica Nacional, de forma tal, que permita el aseguramiento de su disponibilidad e integridad de manera permanente.

Artículo 23. Suministro de energía. El equipo informático requiere ser protegido ante las posibles fallas en el suministro de energía y otras anomalías eléctricas. El suministro eléctrico debe ser acorde con las especificaciones del fabricante o proveedor de cada equipo. Para esto, la administración dota a las diferentes dependencias de los materiales necesarios para el cumplimiento de estas especificaciones.

Artículo 24. Seguridad del cableado. El cableado de energía eléctrica y de comunicaciones, que transporta datos o brinda apoyo a los servicios de información, requiere mantenerse protegido contra intercepción o daño.

Artículo 25. Identificación de bienes. Es deber de la Dirección de Control de Bienes e Inventarios, identificar los activos de tecnologías de la información de la Universidad (tangibles e intangibles) y asignar personas responsables. Dichos equipos son conectados a la red interna; en caso contrario, se genera un requerimiento de excepción, dado que los equipos ajenos a la Institución no pueden conectarse a la Red Institucional.

Artículo 26. Entrega de bienes de tecnologías de la información. Toda persona que culmine su vínculo con la Universidad o se den cambios que lo ameriten, deben entregar los activos asignados a la jefatura de la unidad administrativa en la cual labora. Es responsabilidad de la jefatura, comunicar a la Dirección de Control de Bienes e Inventarios para realizar los procedimientos de asignación a la nueva persona usuaria, como respaldos, asignación de contraseñas y similares.

Artículo 27. Controles físicos de entradas. Es deber de las jefaturas involucradas proteger las áreas de acceso restringido, mediante controles de ingreso, que aseguren, únicamente,el acceso a las personas autorizadas.

Artículo 28. Acceso restringido. La Dirección de Gestión de Tecnologías de la Información es la responsable de establecer controles y lineamientos de acceso físico y lógico a la información, para las

personas que laboran en áreas restringidas, así como para las actividades de terceros que tengan lugar allí.

Artículo 29. Gestión de desecho y reutilización segura de los equipos. La Dirección de Gestión de Tecnologías de la Información, en colaboración con la Dirección de Control de Bienes e Inventarios, definen los procedimientos para que la información no se vea comprometida por el retiro o reutilización de equipo de tecnologías de información. Los medios de almacenamiento que contienen material sensible, por ejemplo, discos duros no removibles, son físicamente destruidos o sobrescritos en forma segura, en lugar de utilizar las funciones de borrado estándar, según corresponda.

Artículo 30. Seguridad perimetral. Toda información sensible requiere ser gestionada, de acuerdo con las Normas de Archivo Institucional en lo referente al acceso restringido y seguro, mediante controles de entrada adecuados. Los controles son alineados a los riesgos identificados de la información; además, de estar claramente establecidos y orientados a crear perímetros de seguridad alrededor de los lugares, donde se resguarda la información o tienen lugar los procesos de información sensible para la Universidad.

CAPÍTULO VI
SEGURIDAD EN LAS OPERACIONES Y COMUNICACIONES

Artículo 31. Identificación del equipo en la red. Los equipos tecnológicos propiedad de la Universidad son debidamente identificados en la red de comunicación de datos de la institución, como medio para administrar y controlar las conexiones.

Artículo 32. Documentación de procedimientos operativos. Es deber de la Dirección de Gestión de Tecnologías de la Información, documentar y mantener actualizados todos los procedimientos de operación en un lugar de fácil acceso para las personas autorizadas.

Artículo 33. Correo electrónico. El uso del correo electrónico está sujeto a las normas y procedimientos que la Universidad especifique. Esto con el fin de que la información que viaja mediante redes públicas, sea protegida de actividad fraudulenta y modificación no autorizada, entre otros.

Artículo 34. Administración de Internet. El acceso a Internet provisto a la población de trabajadores de la Universidad Técnica Nacional, es de uso exclusivo para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas. Es responsabilidad del Área de Gestión Técnica de la Dirección de Gestión de Tecnologías de la

Información, monitorear permanentemente dicha red, para tal efecto, es deber ejecutar tareas y procedimientos que aseguren el uso y explotación óptima de los servicios.

Artículo 35. Transacciones electrónicas. Toda información, que implica el uso de transacciones electrónicas, requiere ser protegida para prevenir la transmisión incompleta, ruta equivocada, alteración no autorizada de mensajes, acceso no autorizado, duplicado no autorizado del mensaje o reproducción. Es deber de la Dirección de Gestión de Tecnologías de la Información proveer la utilización de canales seguros para dichas transacciones.

Artículo 36. Informática móvil y comunicaciones. La Universidad establece los controles, a través de medidas de seguridad apropiadas, para proteger contra los riesgos de utilizar medios informáticos y comunicación móviles. Es deber incluir estas medidas en la utilización segura y eficiente de las redes inalámbricas.

Artículo 37. Gestión de respaldo y recuperación de información. La Dirección de Gestión de Tecnologías de la Información establece procedimientos rutinarios para lograr una estrategia de respaldo eficaz para la recuperación de datos.

Artículo 38. Protección ante software malicioso. Es deber de la Dirección de Gestión de Tecnologías de la Información implementar controles de detección, prevención y recuperación, para evitar ataques mediante código malicioso.

Artículo 39. Gestión de controles de acceso a la red. Los accesos controlados a los recursos de la red son para la prevención de acceso no autorizado, por parte de personas usuarias internas o externas. El acceso a sistemas de información, computadores y periféricos son restringidos, a menos que la jefatura de instancia autorice, explícitamente, mediante excepción. En todo caso, los equipos o periféricos por conectar son alineados a controles de seguridad, establecidos por las áreas respectivas, cuyo fin es verificar el cumplimiento de los requisitos mínimos de seguridad para todo equipo que se conecte a la red institucional.

Artículo 40. Actualizaciones de seguridad. Las actualizaciones de seguridad provistas por fabricantes de software en operación, equipos de trabajo para la atención de emergencias informáticas de centros oficiales y otros terceros, debidamente acreditados, requieren ser evaluadas por las personas responsables de la información, a fin de determinar su aplicación y establecer prioridades, con el propósito de asegurar la

información. Adicionalmente, es deber de la Dirección de Gestión de Tecnologías de la Información establecer el procedimiento estricto de gestión de cambios.

Artículo 41. Teletrabajo. En el momento en que la Dirección de Gestión de Desarrollo Humano, considere pertinente implementar algún tipo de trabajo remoto para la población universitaria o personas externas que requieren acceder a los sistemas de información y alineados a la Ley para regular el Teletrabajo (Ley N°9738), es deber de la jefatura de la instancia coordinar con la Dirección de Gestión de Tecnologías de la Información las medidas de seguridad necesarias, según normativa y políticas vigentes.

Artículo 42. Gestión de instalaciones externas. En el caso de tercerizar la administración de los centros de comunicación o data center, es deber de las jefaturas involucradas, diseñar e incorporar controles con el proveedor del servicio en el contrato.

Artículo 43. Segregación en las redes. Los grupos de servicios de información, de personas usuarias y sistemas necesitan ser segregados en las redes.

Artículo 44. Información pública disponible. La integridad de la información disponible en los sistemas públicos electrónicos tienen que ser protegidos para prevenir modificaciones no autorizadas.

Artículo 45. Gestión de Información. La administración definirá los procedimientos para el manejo y almacenamiento de la información y protegerla de manipulación no autorizada.

Artículo 46. Gestión para nuevos dispositivos de almacenamiento. La administración define e implementa el proceso de autorización para el uso, eliminación y manejo de nuevos dispositivos para el almacenamiento de información.

CAPÍTULO VII
CONTROL DE ACCESO

Artículo 47. Monitoreo en el uso de sistemas. La administración define e implementa los procedimientos para el monitoreo del uso de las instalaciones de procesamiento de la información, con el fin de garantizar que la población universitaria solo esté desempeñando actividades que hayan sido autorizadas.

Artículo 48. Utilización de los servicios de red. La administración controla el acceso a los servicios de red sean internos o externos, como

garante de que la población que tenga acceso a las redes y a sus servicios, no comprometa su seguridad.

Artículo 49. Autenticación de usuarios para conexiones externas. El acceso de personas, de forma remota, está sujeto al cumplimiento de procedimientos de autenticación.

Artículo 50. Administración de privilegios. Es deber de la jefatura de la instancia dueña de la información, eliminar y controlar la asignación y uso de privilegios bajo el principio de “necesidad de saber o menor privilegio”. Los sistemas multiusuario, que requieren protección contra accesos no autorizados, proveen una asignación de privilegios controlada mediante un proceso de autorización formal

Artículo 51. Acceso a los archivos y documentos físicos. El acceso a la información y documentos físicos están estrictamente controlados, asegurando que sólo las personas autorizadas tengan acceso a la información sensible, en concordancia con las normas establecidas por el Sistema Universitario de Gestión Documental.

Artículo 52. Anulación de privilegios de acceso. La Dirección de Gestión de Tecnologías de la Información es la responsable de anular, en cualquier momento, los derechos de acceso a recursos de tecnologías de información, amparada en una causa justificada de compromiso de la seguridad de la información.

Artículo 53. Equipo de atención ante problemas de seguridad de la información. La Dirección de Gestión de Tecnologías de la Información autoriza la aplicación de las medidas correspondientes al equipo de atención de seguridad informática, ante cualquier tipo de incidente que ponga en riesgo la seguridad de la información.

Artículo 54. Monitoreo de privilegios. Es deber de la Dirección de Gestión de Tecnologías de la Información, restringir y monitorear el acceso a los sistemas de información, en colaboración con la jefatura de la instancia correspondiente para identificar potencial uso inapropiado de sistemas e información.

Artículo 55. Acceso al ambiente de producción. El acceso al ambiente de producción es autorizado por las personas responsables de las

oficinas que produzcan la información. El acceso a este ambiente está restringido a la población definida por la instancia.

Artículo 56. Restricción para el tiempo en uso de aplicaciones. El uso de aplicaciones está restringido en razón de minimizar los riesgos en su utilización.

Artículo 57. Control de dispositivos móviles. Cuando la Dirección General Administrativa Universitaria autoriza el uso de dispositivos móviles externos, la persona responsable se ajusta a los lineamientos y estándares establecidos por la Dirección de Gestión de Tecnologías de la Información.

Artículo 58. Intercambio de información y software. Es deber de la administración, establecer acuerdos para el intercambio de información y software que aseguren el uso de los medios de comunicación idóneos entre la Universidad y entidades externas.

Artículo 59. Registro de personas usuarias. Corresponde a la Dirección de Gestión de Desarrollo Humano, emitir un procedimiento para comunicar a la Dirección de Gestión de Tecnologías de la Información de los ingresos y egresos de las personas servidoras de la Universidad Técnica Nacional a los sistemas de información, bases de datos y servicios de información multiusuario.

Artículo 60. Control de enrutamiento en la red. La Dirección de Gestión de Tecnologías de la Información define e implementa controles de enrutamiento, los cuales garanticen, que las conexiones entre computadoras y los flujos de información, no incumplan con el control de acceso establecido para las aplicaciones.

Artículo 61. Control de conexión a la red. Se restringe la capacidad de conexión de las personas que comparten todas las necesidades de transmisión (redes compartidas), en especial aquellas que se extienden más allá de los límites de la institución, en concordancia con el control de acceso.

Artículo 62. Administración de accesos de persona usuaria. Es deber del área involucrada autorizar el acceso a todo sistema por la persona responsable de la información; además, agregar el detalle de dichos accesos y registrarlos en una lista de control de accesos. Tales registros son considerados documentos de acceso restringido.

Artículo 63. Protección del puerto de diagnóstico remoto. Es deber del área de infraestructura y telecomunicaciones restringir y monitorear

el acceso físico y lógico para el diagnóstico y configuración de puertos remotos.

Artículo 64. Acceso a la administración de los sistemas operativos. El acceso a la administración de los sistemas operativos se limita a las personas autorizadas para la ejecución de funciones de administración del sistema. En el caso de los sistemas operativos, bajo la custodia de la Dirección de Gestión de Tecnologías de la Información, tal acceso se realiza con la aprobación específica de los responsables de las áreas de infraestructura y de seguridad; en otros casos, la aprobación es otorgada por la jefatura inmediata correspondiente.

Artículo 65. Administración de contraseñas críticas. Las cuentas de personas usuarias de poco uso, utilizadas únicamente, ante una necesidad específica para realizar alguna tarea que así lo requiera, es requisito estar protegida por una contraseña con un mayor nivel de complejidad.

Artículo 66. Administración de contraseñas de persona usuaria. La selección de contraseñas, su uso y administración como medio de control de acceso primario a los sistemas, debe apegarse a las mejores prácticas. En particular, en ningún caso, las contraseñas se comparten con otra persona. Es deber de toda persona que mantenga relación con la Universidad, seguir buenas prácticas de seguridad en la selección, uso y custodia de claves.

Artículo 67. Verificación de derechos de acceso. Los derechos de acceso asignados a la población universitaria son revisados al menos una vez al año, por parte de la jefatura de la instancia; en colaboración con la Unidad de Seguridad, mediante un procedimiento formal que permita verificar el estado actual de dichos privilegios.

Artículo 68. Control de acceso remoto. Los procedimientos de control de acceso remoto proveen protecciones adecuadas, mediante identificación robusta, autenticación y técnicas de cifrado.

Artículo 69. Control de acceso para trabajo remoto. Es deber de la Dirección de Gestión de Tecnologías de la Información realizar procedimientos de control de acceso, para las personas que laboran bajo la modalidad de teletrabajo y establecer registros de acciones específicas para el control de accesos.

Artículo 70. Acceso no autorizado. Cuando se descubra que una persona ingresa a un sistema o información a la cual no tiene derechos de lectura, escritura, entre otros, el personal del área Seguridad de la

Dirección de Gestión de Tecnologías de la Información, en coordinación con los responsables del sistema o áreas afectadas, están en la obligación de tomar acciones inmediatas para interrumpir el acceso e iniciar la recolección de evidencias de la situación detectada y presentar el informe al Director de la Dirección de Gestión de Tecnologías de la Información y a la jefatura de la dependencia involucrada en el plazo de tres días hábiles, para que se tomen las acciones pertinentes.

CAPÍTULO VIII
SEGURIDAD EN LA IMPLEMENTACIÓN Y MANTENIMIENTO DE SOFTWARE E INFRAESTRUCTURA TECNOLÓGICA

Artículo 71. Seguridad en los sistemas de información. Para evitar la pérdida, modificación o uso inadecuado de datos en los sistemas de información, la jefatura del área involucrada, en colaboración con la Dirección de Gestión de Tecnologías de la Información, establecen controles y registros de auditoría, en la que se valide la entrada y salida de datos, el procesamiento interno y la autenticación de mensajes.

Artículo 72. Verificación en cambios de software y sistemas de información. Es deber de la Dirección de Gestión de Tecnologías de la Información establecer un procedimiento de control formal, para realizar cambios al software y a los sistemas de información. Los cambios realizados se autorizan y aprueban, únicamente, por la persona responsable de la información antes de pasar al ambiente de producción. El procedimiento de control de cambios se utiliza para cualquier modificación al software o sistema de información. Todos los cambios, así como configuraciones que afecten su seguridad y aplicación de actualizaciones, son autorizados y probados antes de pasar al ambiente de producción.

Artículo 73. Separación de ambientes de prueba, desarrollo y producción. La separación de los recursos para el desarrollo, prueba y producción son utilizados para la reducción de riesgos y modificaciones en el sistema operacional no autorizados.

Artículo 74. Planificación del desarrollo de nuevos sistemas. Para el desarrollo de nuevos sistemas o aplicaciones, la Dirección de Gestión de Tecnologías de la Información, supervisa y adapta el uso de recursos, así como tener proyecciones de requisitos futuros para la mejora en su capacidad de operación y optimización.

Artículo 75. Desarrollo externo del software. Todo desarrollo de software por parte de terceros, es supervisado y monitoreado por el área

correspondiente de la Dirección de Gestión de Tecnologías de la Información, con el fin de garantizar el uso correcto de la metodología para el desarrollo de aplicaciones o sistemas, en el cumplimiento de los requisitos de seguridad y de la relación contractual.

Artículo 76. Instalación de software en producción. La Dirección de Gestión de Tecnologías de la Información define los controles necesarios para comprobar la seguridad de la instalación de software en producción.

Artículo 77. Análisis y especificaciones de los requerimientos de seguridad. Todo sistema nuevo o mejora de los existentes sean propios o externos deben contar con los requerimientos de seguridad que la Dirección de Gestión de Tecnologías de la Información considere pertinente.

Artículo 78. Comprobación del inventario de software. Es deber de la Unidad de Aprovisionamiento de la Dirección de Gestión de Tecnologías de la Información, mantener un inventario de software actualizado, de manera que se pueda identificar: la cantidad en existencia, su ubicación física y la persona responsable del uso.

Artículo 79. Verificación de aplicaciones y sistemas críticos. Cuando se realizan cambios en los sistemas operativos, la persona responsable de la aplicación o sistema de información realiza las pruebas necesarias y da, de manera escrita, su aprobación para que no exista un impacto adverso en la operatividad y seguridad de los datos.

Artículo 80. Acceso a las librerías de software. El acceso y actualización de librerías de programas, fuentes y ejecutables entregados, es realizado por profesionales técnicos especializados y autorizados, siguiendo una combinación de controles de acceso técnico y de procedimientos de operación robusta.

Artículo 81. Verificación de versiones de software. Es deber de la Dirección de Gestión de Tecnologías de la Información, utilizar un procedimiento formal para el control comprensivo de las diferentes versiones de los programas y sistemas operativos.

Artículo 82. Desarrollo de software. El software desarrollado por o para la Universidad Técnica Nacional con recursos internos o mediante contratación externa, requiere de un procedimiento formal de desarrollo proporcionado por la Universidad, el cual es administrado desde el mismo proyecto . La integridad del código del software operacional de la

Universidad es protegida utilizando una combinación de controles de acceso técnico y privilegios restrictivos.

Adicionalmente, en el caso de contratación de servicios externos de consultoría, es deber de la Dirección de Proveeduría Institucional, garantizar, mediante la firma de un contrato de confidencialidad, la propiedad del código y protección de la información, así como protegerse del manejo y uso inadecuado que pueda darse a ésta por parte de terceras personas no autorizadas. Los cambios propuestos al software son convenidos y autorizados por la persona propietaria de la aplicación, siendo ésta la persona responsable del impacto.

Artículo 83. Aprobación de sistemas o aplicaciones. La Dirección de Gestión de Tecnologías de la Información establece los criterios de aceptación para nuevos sistemas de información, versiones nuevas o mejoradas y desarrollar con ellos, las pruebas adecuadas antes y durante su aceptación.

Artículo 84. Correcciones de emergencia al software. La persona responsable de la información, en conjunto con la Dirección de Gestión de Tecnologías de la Información, definen cuando una corrección es crítica y de aplicación urgente. Cualquier cambio o corrección al software sigue estrictamente el procedimiento de control de cambios definido por la universidad.

Artículo 85. Entrada del personal técnico a los sistemas en producción. El acceso a la funcionalidad de los sistemas en producción, así como en sus bases de datos, mediante el uso de aplicaciones propias u otro medio o herramienta informática, es restringido y autorizado, por escrito, por la persona responsable de la información. No se permite este tipo de acceso a las personas con conocimiento técnico, entendiéndose desarrolladores, analistas de sistemas, programadores, soporte técnico, contrapartes, administradores del sistema, gestores de bases de datos, proveedores externos o empresas y, en general, cualquiera cuya función no sea propiamente del área funcional autorizado de los sistemas, aplicaciones y bases de datos en producción.

CAPÍTULO IX
CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN

Artículo 86. Regulación del proceso de continuidad. Es deber de la Dirección de Gestión de Tecnologías de la Información mantener un plan de contingencias actualizado, así como un control de criticidad de los activos de tecnologías de la información.

Artículo 87. Gestión de planes de contingencias informáticas. Para los sistemas informáticos en producción y las redes de comunicación, es deber de la Dirección de Gestión de Tecnologías de la Información disponer de un plan de contingencia, el cual es actualizado y probado regularmente, con el fin de garantizar la continuidad de los procesos críticos de la Universidad, en caso que se presente una interrupción o degradación del servicio.

Artículo 88. Ataque a los sistemas. Cuando se detecta que un sistema ha sido comprometido, el hardware involucrado es inmediatamente removido de la red y se siguen todos los procedimientos para asegurar que el sistema está libre de compromisos antes de la reconexión. Cuando la fuente o un punto intermedio de un ataque a los sistemas ha sido debidamente identificado, el hardware en cuestión debe ser aislado del entorno de red para evitar mayor compromiso a los recursos de la red y de los sistemas en producción. Además, se procede conforme con el plan de contingencia establecido por el área a cargo de la administración del equipo y de los servicios que este brinda.

Artículo 89. Incidentes de seguridad de la información. La Dirección de Gestión de Tecnologías de la Información establece las responsabilidades y procedimientos generales administrativos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información, así como una adecuada documentación de aprendizaje. Por otra parte, se requiere que existan mecanismos que permitan la cuantificación del daño y seguimiento a los tipos, volúmenes y costo de los incidentes en materia de seguridad de la información.

Artículo 90. Equipo de atención de emergencias informáticas. La Dirección de Gestión de Tecnologías de la Información es responsable de organizar y mantener un equipo de atención de emergencias informáticas, el cual tenga la capacidad de brindar una respuesta organizada y ágil a los problemas contingentes que se puedan manifestar en los servicios, los cuales prestan los sistemas críticos, ofreciendo una evaluación de los daños y proponiendo opciones de corrección que sean factibles de ejecutar en el corto plazo.

Artículo 91. Simulaciones de atención de emergencias informáticas. La Dirección de Gestión de Tecnologías de la Información define y coordina la realización de incidentes simulados para movilizar y probar la eficacia del equipo de atención de emergencias informáticas y sus procedimientos.

Artículo 92. Análisis de impacto. Producto del análisis institucional de evaluación de riesgos, la persona responsable de la información,

específica el tiempo en el que puede operar sin procesamiento de información crítica, el período de tiempo antes de movilizar sus operaciones bajo el modelo de contingencia y la configuración mínima aceptable para la operación.

Artículo 93. Notificación de vulnerabilidades. Es deber de la Unidad de Seguridad revisar los avisos de vulnerabilidad emitidos, periódicamente, por organizaciones internacionales especializadas y confiables, realizando oportunamente las recomendaciones que estimen necesarias para que se tomen las previsiones técnicas pertinentes, por parte de las áreas responsables de la administración y operación de los recursos tecnológicos de nivel institucional.

Artículo 94. Comunicación de incidentes de seguridad. Es deber de la Dirección de Gestión de Tecnologías de la Información establecer, mantener y probar, un procedimiento que les permita a las personas funcionarias reportar incidentes de seguridad. Dicho procedimiento, especifica los roles y responsabilidades para los individuos responsables por el manejo de incidentes de seguridad de información.

Artículo 95. Esquema de clasificación de la información. Es deber clasificar la información en una de las tres categorías de criticidad, cada una con requerimientos separados de manejo. Estas categorías son las siguientes: Pública, Interna y Restringida, según se establece en el documento Esquema de Clasificación de la Información (1.4.1 DGTI-EA-0116), el cual se encuentra en el sitio oficial de la Dirección de Gestión de Tecnologías de la Información. Esta tarea es realizada periódicamente entre los responsables de la información y la Dirección de Gestión de Tecnologías de la Información.

Artículo 96. Valoración en la prioridad de recuperación de aplicaciones multiusuario. Es deber de la Unidad de Infraestructura y Comunicaciones, establecer y utilizar un esquema lógico para la clasificación de los recursos de información por prioridad de recuperación, el cual permita que los recursos más críticos se recuperen primero.

Artículo 97. Roles y responsabilidades en la planificación de contingencias y recuperación de sistemas. Los roles y responsabilidades para la planificación de contingencias y la recuperación de sistemas son revisados periódicamente por la administración de seguridad de la información, la cual es responsable de hacer las observaciones que estime pertinentes.

CAPÍTULO X

CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD

Artículo 98. Controles de auditoría de sistemas. Cuando las jefaturas de área, en colaboración con la Dirección de Gestión de Tecnologías de la Información, realizan actividades de control y seguimiento que involucran la verificación de los sistemas en producción, es deber tomar precauciones en la planificación de los requerimientos y tareas acordadas con las áreas involucradas, a efectos de minimizar el riesgo de interrupciones en las operaciones.

Artículo 99. Protección de los elementos utilizados por la auditoría de sistemas. La administración, en colaboración con la Dirección de Gestión de Tecnologías de la Información, son los responsables de proteger el acceso a las herramientas de supervisión y control dispuestas en los sistemas, sea archivos de datos o software, a fin de evitar el mal uso o su compromiso. Dichas herramientas permanecen separadas de los sistemas en producción y de desarrollo y se les otorga el nivel de protección requerido.

Artículo 100. Acatamiento de la política de seguridad de la información. La población universitaria y terceros, que realizan labores técnicas o funcionales en relación con los sistemas informáticos, tienen la estricta obligación de conocer y cumplir con los lineamientos y disposiciones de seguridad de la información contenidas en las políticas institucionales. Es deber de las jefaturas de área velar por su cumplimiento, so pena de incurrir en responsabilidad administrativa, civil o penal.

Artículo 101. Uso de información y documentación relacionada con sistemas informáticos. La información generada o producida por los sistemas informáticos en producción y documentos relacionados, no puede ser reproducida o utilizada sin el permiso de la persona responsable de la información.

Artículo 102. Registro de evidencias de Incidentes. Toda la información, que sirva como evidencia para documentar incidentes de seguridad, tiene que estar formalmente registrada y comunicada de manera verbal o por escrito al funcionario de seguridad a cargo o al jefe inmediato.

CAPÍTULO XI
RESPONSABILIDADES Y SANCIONES

Artículo 103. Responsabilidad por incumplimiento del presente reglamento. En caso de incumplimiento de los lineamientos establecidos en el reglamento de seguridad, las presuntas personas responsables pueden ser sometidas a un proceso administrativo o lo que

corresponda, según las regulaciones universitarias vigentes y a cualquier otra normativa nacional.

Artículo 104. Sanciones. Pretenden generar y afianzar una cultura de seguridad de la información entre las personas, que por la naturaleza de su relación con la Universidad utilizan las tecnologías de información dispuestas por la Institución. Por tal razón, es necesario que las faltas sean clasificadas con el objetivo de aplicar las medidas correctivas.

Faltas leves: Corresponde a las faltas no contempladas en faltas graves o muy graves y que no impactan de forma inmediata la información y las tecnologías relacionadas:
a. No comunicar, de forma pronta y oportuna, a la Dirección de Gestión de Tecnologías de la Información un incidente de seguridad.
b. Que la persona usuaria no haga uso de los recursos informáticos, en atención a las disposiciones establecidas en el presente reglamento.
c. La conexión de equipos a la red institucional sin autorización de la Dirección de Gestión de Tecnologías de la Información.
Faltas graves: Trata las transgresiones de seguridad de las Tecnologías de la Información y la Comunicación que impactan directamente la disponibilidad, integridad y confidencialidad de estas.
a. Omitir procedimientos para el otorgamiento de roles y permisos a las personas usuarias.
b. La persona responsable no acate las soluciones que indica la Dirección de Gestión de Tecnologías de la Información ante la gestión de una incidencia.
c. No custodiar, los recursos informáticos que se le han asignado.
d. Acceso físico o lógico no autorizado.
e. Instalación de software no autorizado por la Dirección de Gestión de Tecnologías de la Información.
f. La notificación de tres faltas leves en un periodo inferior a un año.

Faltas muy graves: Son las originadas por la falta de adopción de las medidas de seguridad, orientadas a subsanar los incumplimientos detectados.
a. Robo de información.
b. Omitir, por segunda vez, el acatamiento de las medidas de seguridad indicadas por la Dirección de Gestión de Tecnologías de la Información.
c. El ocultamiento de actividades malintencionadas de cualquier persona, en perjuicio de la disponibilidad, integridad y confidencialidad de la información.
d. Suplantación de identidad y fraude.
e. Recibir dos notificaciones de faltas graves en un periodo inferior a un año.

Artículo 105. Vigencia y derogación del reglamento. Este reglamento rige a partir de su publicación y deroga, de manera expresa, cualquier normativa o disposición que lo contradiga.

(Aprobado mediante Acuerdo 11-15-2022, tomado por el Consejo Universitario en la Sesión Ordinaria No. 15-2022, celebrada el jueves 14 de julio del año 2022, a las nueve horas, según el Artículo 20 del Capítulo XI. Comisión Interna de Reglamentos. Publicado en el diario oficial La Gaceta No. 152 del 11 de agosto del año 2022, sección de Reglamentos).

EDGAR ALEJANDRO SOLIS MORAGA (FIRMA)

Firmado digitalmente por EDGAR ALEJANDRO SOLIS MORAGA (FIRMA)
Fecha: 2022.08.22 16:58:07 -06'00'