CIRCULAR INSTRUCCIÓN
UNA-DTIC-DISC-006-2021

PARA Asamblea de Representantes, Consejo Universitario, CONSACA, Rector, Rectora Adjunta, Vicerrector(as), Decanos(as), Vicedecanos(as), Directores(as) y subdirectores (as) de unidades académicas y sección regional, Directores (as) Ejecutivos(as) de Facultad, Centro y Sede, Directores(as) y jefaturas de instancias de apoyo a la academia, Profesionales Ejecutivos(as) de Unidades Académicas, Administrativas y Paraacadémicas, Presidentes(as) de Órganos Desconcentrados, y Comunidad Universitaria en general.

DE Dirección de Tecnologías de la Información y la Comunicación (DTIC).

FECHA 25 de octubre de 2021

ASUNTO: RECORDATORIO INSTRUCCIONES PARA SEGURIDAD DE LA INFORMACION INSTITUCIONAL Y SEGURIDAD TECNOLOGICA.

PRIMERO: MARCO JURIDICO:

1. Constitución Política de Costa Rica, artículos 24, 27 y 30.
2. Ley General de Administración Pública.
3. Ley de Control Interno.
4. Ley de Regulación del Derecho de Petición, Ley 9097 del 26/10/2012
5. Ley de Protección al ciudadano del exceso de requisitos y trámites administrativos, Ley 8220 del 04/03/2002
6. Ley Nº 8968 del 7 de julio del 2011, Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.
7. Estatuto Orgánico de la Universidad Nacional, articulo 1.b
8. Política Institucional para la Promoción de la Ética en la UNA, numerales XXV y XXVII.
9. Políticas para la Utilización de los Servicios Electrónicos Brindados por la UNA, Disposición General 3 y 6 y numeral 10 del apartado Sobre Correo Electrónico.
10. Reglamento del Sistema de Mejoramiento Continuo de la Gestión Universitaria, artículos 40, 41 y 42.
11. Las Normas Técnicas Institucionales para la Gestión y el Control de las Tecnologías de la Información y Comunicación, numerales 1.4, 1.7 Y 4.3
12. Reglamento Para la Emisión de Normativa Universitaria, art. 3 inciso f.
13. Matriz de SISTEMATIZACIÓN DE LA INFORMACIÓN INSTITUCIONAL EN IRRESTRICTA, RESTRINGIDA, DATOS SENSIBLES, PÚBLICA Y CONFIDENCIAL

SEGUNDO: ALCANCE

Estas instrucciones son de acatamiento obligatorio para todas las autoridades y personal universitario y tienen como objetivo garantizar la seguridad de la información institucional existente en todo tipo de archivo, repositorio o base de datos institucional. Además, establece disposiciones generales y vinculantes para el uso y resguardo del equipo en el cual se incluye, procesa y resguarda la información institucional y el uso de contraseñas.

Lo anterior, con el objetivo de lograr un sano equilibrio entre los derechos constitucionales y legales del personal universitario, los usuarios y del público en general que se relaciona y brinda información a la institución, el acceso a la información pública por parte de cualquier interesado y el uso y análisis de la información para la toma de decisiones para la gestión de la acción sustantiva institucional.

Finalmente, esta instrucción constituye un medio para garantizar razonablemente la seguridad de la información, y para garantizar que es usada y/o modificada únicamente por personal autorizado.

TERCERO: INSTRUCCIONES

I. COMPROMISO CON LA TRANSPARENCIA, LA ENTREGA DE LA INFORMACIÓN, LA SEGURIDAD DE LOS DATOS Y EL RESPETO AL DERECHO A LA INTIMIDAD (DATOS PERSONALES Y CONFIDENCIALES).

1. La Universidad Nacional, como parte de su compromiso con la transparencia cuenta con portales y sitios web abiertos al público, por medio de los cuales pone a disposición de cualquier interesado (interno o externo a la institución), la información pública y de acceso irrestricto, entre los principales se indican como referencia los siguientes:

   1.1. Sitio de Transparencia - https://www.transparencia.una.ac.cr/
   1.2. Portal de revistas electrónicas – https://www.revistas.una.ac.cr/
   1.3. Repositorio académico - https://repositorio.una.ac.cr/
   1.4. Repositorio de documentos - http://documentos.una.ac.cr/
   1.5. Sitio oficial de comunicación - https://www.unacomunica.una.ac.cr/
   1.6 Sitio Web Institucional - https://www.una.ac.cr/
   1.7 Sitio Web Comisión Institucional de Teletrabajo - www.teletrabajo.una.ac.cr
   1.8 Sitios Web de instancias universitarias.

2. Toda persona interesada en acceder a información no incluida en el punto anterior debe solicitarla ante el superior jerárquico de la instancia responsable de la administración de esa información.

3. Toda autoridad o funcionario que reciba una solicitud de información que no es de su competencia debe trasladarla, de inmediato, a la instancia competente e informar del traslado al solicitante.

4. La Dirección de Tecnologías (DTIC) como parte de sus funciones es la responsable de custodiar y garantizar la preservación de la información almacenada en los sistemas de información y plataformas tecnológicas que administra. Las solicitudes de información deben gestionarse a través de la instancia responsable del proceso que la genera.

5. Todo superior jerárquico debe entregar a la persona solicitante, **la información pública** o de **acceso irrestricto** que tenga en los archivos, repositorios y bases de datos bajo su responsabilidad.

   En caso de que lo solicitado sea información de **acceso restringido**, **datos sensibles** o **información confidencial** debe comunicar la imposibilidad de la entrega al solicitante, por escrito y con la correspondiente explicación de los motivos y normas que justifican su decisión.

   La información o comunicación de la no entrega debe hacerse a la brevedad posible. Cuentan con un plazo máximo de 10 días hábiles. En caso de que la entrega de la información, por su complejidad requiera de un plazo mayor, se debe informar del motivo y el plazo razonable en el cual se hará efectiva la entrega, dentro de los 10 días hábiles antes indicados.

6. Considerando la legislación nacional, la normativa institucional y los criterios jurídicos (UNA-AJ-CJUR-283-2017, AJ-D-224-2015, UNA-AJ-DICT-017-2020) emitidos por la Asesoría Jurídica, la información existente en los archivos, repositorios y bases de datos institucionales se clasifican de la siguiente forma:

6.1 Información que contiene datos sobre personas:

6.1.1 **Datos sensibles**: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros. Esta información no puede ser brindada a ninguna instancia o persona externa o interna.

6.1.2 **Datos de acceso restringido**: los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Su entrega solo será permitida para fines públicos o si se cuenta con el consentimiento expreso del titular.

6.1.3 **Datos de acceso irrestricto**: los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.

6.2 Información institucional que no tiene datos de personas:

6.2.1 **Información Pública**: información sobre el funcionamiento y el quehacer institucional que es de acceso irrestricto para cualquier interesado. Es toda la información que no sea clasificada como confidencial por la organización.

6.2.2 **Información Confidencial**: información que debe ser resguardada por la institución, a la cual solamente tendrán acceso personal específico de la institución, ya que lo contrario implica un riesgo a la seguridad financiera, informática, tecnológica o estructural de la institución.

6.3 Específicamente con relación a **la Información Confidencial relacionada con la seguridad tecnología e informática**, se refiere a aquella que carece de valor informativo y su publicación representa riesgos y amenazas para la continuidad de la plataforma tecnológica y la confidencialidad de la información. En esta categoría se clasifica la siguiente información:

6.3.1 Contraseñas de equipos que no son de uso personal.
6.3.2 Direcciones IP de servidores o plataforma tecnológica institucional.
6.3.3 Información que garantice la seguridad de las bases de datos y aplicaciones.
6.3.4 Información que facilite el acceso a la plataforma tecnológica diferente a la que tiene acceso el usuario.
6.3.5 Código fuente.
6.3.6 Ubicación de centro de datos y activos de información críticos.
6.3.7 Personal con acceso o responsable de administrar la plataforma tecnológica.

7. Para facilitar a los superiores jerárquicos el análisis del tipo de información que se está solicitando y contar con seguridad jurídica en la toma de las decisiones, se pone a disposición de la comunidad universitaria la matriz de clasificación de la información institucional publicada en el sitio http://enlaces.una.ac.cr/clasificaciondeinformacion, del repositorio de documentos de la Asesoría Jurídica. En dicha matriz también puede consultarse los proveedores oficiales de información.

   Únicamente si la información solicitada, no está en dicha matriz y se tienen dudas de si la información solicitada es o no publica o de acceso irrestricto, debe consultar a la Asesoría Jurídica al correo asesoria@una.cr.

8. El personal universitario que no tiene un puesto de autoridad no debe compartir información con terceros, ajenos a la institución a la cual tienen acceso por las funciones propias de su cargo, salvo instrucción de su superior jerárquico.

II. COMPROMISO DEL PERSONAL UNIVERSITARIO CON LA SEGURIDAD DE LA INFORMACIÓN INSTITUCIONAL:

1. El personal universitario está obligado a guardar confidencialidad de la información electrónica o impresa a la cuál tienen acceso como parte del desempeño de sus funciones. Deben mantener

discreción sobre la misma y no divulgarla fuera del entorno laboral correspondiente; salvo que su superior jerárquico se lo solicite, y corresponda su entrega.

2. Es responsabilidad del personal universitario proteger la información institucional a la que se le brinda acceso, evitar su sustracción o extravío y garantizar la seguridad de la información de **acceso restringido, datos sensibles e información confidencial** que gestiona la Universidad.

3. El personal universitario puede compartir información a la que tienen acceso por las funciones propias de su cargo, con otros funcionarios e instancias universitarias, siempre y cuando el superior jerárquico se lo instruya previa verificación de la legitimación y finalidad de la solicitud.

III. SEGURIDAD FÍSICA Y AMBIENTAL DE LOS ACTIVOS TECNOLÓGICOS

1. Todo el personal universitario debe cumplir con la regulación institucional establecida para el ingreso y salida de equipos tecnológicos (activos) de las diferentes instancias universitarias.

2. Todas las computadoras institucionales deben contar con un software de antivirus. Para este propósito la DTIC habilita un servicio en su sistema de tiquetes para la instalación y actualización de software (antivirus). El cual será brindado de acuerdo con el licenciamiento institucional disponible y podrá ser utilizado en las computadoras de la institución.

3. La DTIC implementa el uso de herramientas de bloqueo de contenido o accesos no autorizados, como Firewalls, filtradores de contenido y cualquier otra tecnología para favorecer el sistema de seguridad de la red de datos institucional. Lo anterior, como una medida de protección para minimizar los riesgos de ingreso y propagación de software malicioso o virus en la red institucional.

IV. SEGURIDAD INTERNA PARA EL ACCESO DE LA INFORMACIÓN. ACCESOS Y CONTRASEÑAS:

1. La DTIC garantiza que todos los sistemas de información deben contar con mecanismos de autenticación que aseguren la verificación de ingreso y el no repudio de las transacciones realizadas. Excepto cuando se requiera el anonimato para recibir denuncias, quejas o similares.

2. Las contraseñas no deben hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, nombre de usuario, meses del año, nombres de personas, teléfonos o similares.

3. Las contraseñas o claves de acceso a los sistemas de información, para realizar trámites que no son personales, requieren de una solicitud formal, autorizada por el superior jerárquico de la instancia a la que pertenece el funcionario o funcionaria. La solicitud debe especificar claramente los derechos de acceso (roles, menús, procesos) que requiere el usuario respectivo, para tal efecto la DTIC pone a disposición el procedimiento UNA-DTIC-MAPR-002-2018 - Procedimiento Solicitud, Modificación y Actualización de Códigos de Usuario (https://enlaces.una.ac.cr/codigosdeusuario)

4. Los usuarios tendrán acceso únicamente a aquellos datos, aplicaciones y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

5. Los usuarios son responsables de toda actividad realizada con el uso de la cuenta de usuario que le haya sido asignada, por lo que es su responsabilidad custodiar adecuadamente la contraseña y mantener su uso en el ámbito personal.

6. Los usuarios no deben utilizar cuentas de acceso de ningún otro usuario, aunque dispongan de la autorización del propietario.

7. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona, ni mantenerla por escrito a la vista, ni al alcance de terceros.

8. Es obligatorio que el usuario cambie la contraseña provisional asignada por el sistema institucional de autenticación, la herramienta para facilitar este cambio se encuentra en el sitio web institucional (https://www.claves.una.ac.cr/), y el procedimiento puede consultarse en el siguiente sitio: https://enlaces.una.ac.cr/cambioclaveunificada.

9. Los usuarios deben cambiar sus contraseñas de los sistemas institucionales al menos dos (2) veces al año.

10. La longitud mínima de las contraseñas debe ser igual o superior a ocho (8) caracteres, se recomienda utilizar contraseñas de la mayor longitud posible, que puedan ser recordadas para evitar fraudes o vulneraciones. Las contraseñas deben estar constituidas por una combinación de las clases de letras mayúsculas, minúsculas, números o caracteres especiales. La contraseña no debe contener vocales.

Clase	**Descripción de la clase**
Letras Mayúscula	B,C,D… Z
Letras Minúsculas	b,c,d… z
Números	0,1,2,3… 9
Caracteres Especiales	¡!#$%&@.()

11. Los usuarios son responsables de proteger los datos a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

12. Los usuarios son responsables de proteger contra perdida, robo o extravío los documentos electrónicos con los que realizan sus labores diarias, para este fin se recomienda respaldar en medios alternos como discos duros externos, memorias externas tipo USB o similares, adicionalmente la universidad provee soluciones de almacenamiento en nube como Google Drive y Microsoft One Drive, que pueden ser utilizados para este propósito.

13. Toda salida de un activo de información (en soportes informáticos) deberá ser realizada por el personal autorizado y será necesaria la autorización formal del responsable del área de la que proviene.

14. Se prohíbe a los usuarios intentar obtener por medios no oficiales, como hacking, phishing, o ingeniería social, otros derechos o accesos distintos a aquellos que les hayan sido asignados formalmente.

15. Se prohíbe a los usuarios realizar o programar acciones para afectar la disponibilidad, capacidad o seguridad de la plataforma tecnológica o los sistemas de información, mediante técnicas de hacking, ataques de denegación de servicios, o similares.

16. Se prohíbe a los usuarios, realizar cualquier actividad que afecte o comprometa la capacidad, seguridad o disponibilidad de los sistemas y plataformas tecnológicas, como pruebas de stress, análisis de vulnerabilidades, pruebas de penetración o similares.

17. Todo usuario debe hacer uso responsable de los recursos tecnológicos y los servicios que brinda la DTIC a la institución y utilizarlos para el fin para el cual fueron delegados.

V. REGIMEN DE RESPONSABILIDAD:

1. Es responsabilidad de los superiores jerárquicos de todas las unidades académicas, decanatos, órganos desconcentrados, instancias de apoyo a la académica (Programas y Departamentos) y presidencias de los órganos colegiados, que son usuarios y tienen acceso a los sistemas de

información institucional, garantizar la lectura y conocimiento de esta circular instrucción por todo el personal a su cargo.

2. Cualquier vulneración o uso incorrecto de información institucional en forma diferente a lo establecido por la legislación nacional, políticas y reglamentos institucionales y esta instrucción generará responsabilidad administrativa, civil y eventualmente penal.

Atentamente,

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Axel Hernández Vargas, M.Sc.
Director General

Dms