

ARTICULO XVIII: AUDIENCIA M.SC. VIGNY ALVARADO, JEFE DE LA OFICINA DE SISTEMAS

Se atiende la audiencia del Máster Vigny Alvarado, Jefe de la Oficina de Sistemas y Coordinador de la Comisión de Ciencias y Tecnología, quien expone ante este Consejo sobre la Seguridad Digital a nivel institucional y sobre el uso de las claves de acceso, según oficios OS-2000-353 y 403

CONSIDERANDO

- Que las políticas sobre Seguridad Digital se adscriben al principio de eficiencia consagrado en el artículo 4 de la Ley de Contratación Administrativa, en virtud del cual, se persigue con la seguridad digital la satisfacción del interés general y el cumplimiento de los fines y cometidos de la UNED, en lo que respecta a la protección de los bienes que se adquieren. En concordancia con lo anterior y procurando que se administren bien los recursos del Estado y se aproveche debidamente su utilidad resguardándolos de todo daño, es necesario adoptar una política inmediata de seguridad. Esto implica que es imprescindible proteger los recursos y hacer una identificación de las posibles amenazas a las que esos recursos están expuestos, previendo la posibilidad de pérdida total o parcial de los mismos, así como las eventuales causas de daño o perjuicio contra los mismos. **En esta medida, debe tomarse la seguridad digital como una política preventiva y de aplicación inmediata.**
- Que se debe evitar por tanto toda acción negligente que afecte la información de la UNED, como lo es :
 - ❖ El acceso de un tercero por medio del código y clave de otro usuario que descuidó su código, o el acceso no autorizado a las instalaciones de cómputo, a los cuartos o gabinetes de comunicaciones, al cableado o conectores de red, acciones todas que podrían poner en peligro los bienes públicos que custodiamos a nivel material y de información. Por lo tanto es necesario considerar que **el uso de cualquier recurso hacia la red sin la debida o previa autorización se debe identificar como un acceso no autorizado.**
 - ❖ El dar a conocer información valiosa, confidencial o en proceso de trámite, de forma voluntaria o involuntaria, tales como el código de usuario y su clave, código fuente, estructuras de las bases de datos, documentación de análisis o de diseño, diagramas, organización y topología de la red, direccionamiento IP, detalles sobre los sistemas de información o transaccionales.
 - ❖ La programación dañina, capaz de reproducirse por sí sola, o software programado con características eminentemente destructivas, o programas que se multiplican y se redistribuyen con intenciones dolosas y destructivas. Estos programas pueden hacer inservible la red por difusión de paquetes, por inundación de tráfico, expulsión del servicio de uno, varios o de todos los servidores, así como a un enrutador, conmutador o a un segmento de la red. Además usualmente ocasionan pérdida de datos en los pc's y en los servidores. Para contrarrestar estas amenazas es necesario

establecer políticas pertinentes y un plan adecuado de contingencia y de respaldo.

- Que los funcionarios de la UNED, como depositarios de bienes públicos, estamos llamados a ejercer todas las acciones de control y supervisión de aquellos bienes adquiridos con recursos del Estado. Es parte de nuestro deber de diligencia y sana administración, proteger la información sensible, proteger los recursos y tomar toda previsión posible que evite eventuales responsabilidades administrativas, civiles o penales, o bien pérdidas que representen un perjuicio económico para la institución.

SE ACUERDA:

1. Declarar de interés institucional de la UNED y de acatamiento obligatorio las directrices sobre Seguridad Digital que emita la Oficina de Sistemas en resguardo del bien público y la información institucional ubicada en la granja de servidores, y en todos aquellos equipos interconectados en la red institucional "RedUned" y en otros componentes.
2. Declarar de interés institucional y acatamiento obligatorio, las directrices emitidas por la Oficina Jurídica, denominadas "*Copyright*" y "*Aviso Legal*" constantes al pie del portal de la Universidad Estatal a Distancia (www.uned.ac.cr).
3. Declarar de uso individual las contraseñas y códigos de usuario que asigne la Oficina de Sistemas, para lo cual se solicita a todas las Jefaturas y Direcciones de la institución gestionar en el plazo de un mes los códigos de acceso respectivos para el personal a su cargo que utilice recursos tecnológicos.
4. Declarar que la Oficina de Sistemas es la única instancia que puede interconectar equipos a la red institucional y subredes, conceder accesos locales y remotos, y aprobar el uso de la red y sus recursos.
5. Declarar de interés institucional las capacitaciones que brindan sobre seguridad digital e implicaciones legales del uso de la red la Oficina de Sistemas y la Oficina Jurídica.
6. Instar a los funcionarios de la UNED a respetar las políticas de seguridad tendientes a proteger nuestros sistemas de información y los recursos de la universidad
7. Acoger las políticas de seguridad indicadas en el documento "Seguridad Digital", el cual se incorpora a este acuerdo para todos sus efectos.
8. Divulgar ampliamente a la comunidad universitaria los alcances del presente acuerdo por medio de los Consejos de

Vicerrectorías con la participación de la Oficina de Sistemas y la Oficina Jurídica.

9. Coordinar con el Ing. Pablo Cob Saborío, Presidente Ejecutivo del Instituto Costarricense de Electricidad, una reunión conjunta con el M.Sc. Vigny Alvarado Castillo, Jefe de la Oficina de Sistemas de la UNED, con el fin de dar seguimiento a los alcances de la Carta de Intenciones firmada el 12 de abril por el Máster Rodrigo Arias Camacho, Rector de la UNED y el Ing. Róger Echeverría, Subgerente del ICE

Seguridad Digital

Acuerdo tomado por el Consejo de Rectoría en sesión 1160-2000, Art. XVIII

"CONSIDERANDO QUE:

1. La Seguridad Digital pretende proteger diversos recursos en la red.
2. Es interés institucional regular el uso de los servicios que se ofrecen a nuestros usuarios, a través de medidas de seguridad que resguarden los recursos invertidos y los bienes públicos.
3. Existe información sensible y de ingreso restringido que por resguardar los sistemas financieros y técnicos de la UNED y el derecho a la intimidad de nuestros usuarios, debe ser protegida de forma especial.
4. Es interés institucional velar por la inalteración de documentos públicos ofrecidos en la red.
5. Es interés institucional velar por la buena imagen y el buen nombre de la institución
6. Es interés institucional proteger los intereses y derechos de terceros que ingresen como usuarios a la red

POR TANTO, EL CONSEJO DE RECTORÍA ACUERDA:

10. Declarar de interés institucional de la UNED y de acatamiento obligatorio las directrices sobre Seguridad Digital que emita la Oficina de Sistemas en resguardo del bien público y la información institucional ubicada en la granja de servidores, y en todos aquellos equipos interconectados en la red institucional "RedUned" y en otros componentes.
11. Declarar de interés institucional y acatamiento obligatorio, las directrices emitidas por la Oficina Jurídica, denominadas "*Copyright*" y "*Aviso Legal*" constantes al pie del portal de la Universidad Estatal a Distancia (www.uned.ac.cr).
12. Declarar de uso individual las contraseñas y códigos de usuario que asigne la Oficina de Sistemas, para lo cual se solicita a todas las Jefaturas y Direcciones de la institución gestionar en el plazo de un mes

los códigos de acceso respectivos para el personal a su cargo que utilice recursos tecnológicos.

13. Declarar que la Oficina de Sistemas es la única instancia que puede interconectar equipos a la red institucional y subredes, conceder accesos locales y remotos, y aprobar el uso de la red y sus recursos.
14. Declarar de interés institucional las capacitaciones que brindan sobre seguridad digital e implicaciones legales del uso de la red la Oficina de Sistemas y la Oficina Jurídica.
15. Instar a los funcionarios de la UNED a respetar las políticas de seguridad tendientes a proteger nuestros sistemas de información y los recursos de la universidad
16. Acoger las políticas de seguridad indicadas en el documento "Seguridad Digital", el cual se incorpora a este acuerdo para todos sus efectos.
17. Divulgar ampliamente a la comunidad universitaria los alcances del presente acuerdo por medio de los Consejos de Vicerrectorías con la participación de la Oficina de Sistemas y la Oficina Jurídica.

ACUERDO FIRME"