HUMACAO COMMUNITY COLLEGE
Tradición • Excelencia • Transformación

Oficina de Presidencia

787-852-1430
EXT. 224

PO BOX 9139
HUMACAO, PUERTO RICO 00792

POLÍTICA DE SEGURIDAD CIBERNÉTICA

Introducción:

Humacao Community College (la Institución) con la intención de crear esta "Política de Seguridad Cibernética", no para imposición de restricciones, sino para proteger a empleados, profesores, estudiantes y a sí misma, de operaciones totalmente ilegales o que puedan causar algún daño, ya sea una acción consciente o inconscientemente.

Todo lo relacionado a sistemas de información, tal como lo es redes locales, Internet, equipos informáticos, programas (programas de trabajo y sistemas operativos), unidades y medios de almacenamiento, cuentas de directorio activo ("Active Directory"), cuentas de correo electrónico institucional son propiedad de la Institución. Los sistemas de información son estrictamente para ser utilizados con motivos administrativos y educacionales en el mejor interés de la Misión, Visión y Valores.
El esfuerzo en equipo en donde cada integrante de la Institución (dígase profesores, administradores, contratistas, suplidores y estudiantes) tenga acceso a la información de estudiantes y empleados. Cada usuario es responsable de conocer las políticas que apliquen para hacer un uso responsable de todos los equipos de sistemas.

Propósito:

El propósito de esta Política es dar a conocer sobre el manejo responsable de equipos y sistemas de la Institución. En busca de proteger a los empleados administrativos, facultativos, estudiantes y a la Institución misma, ya que el manejo irresponsable puede exponer a la Institución a riesgos, en el cual se incluye infección de virus cibernético donde se pueda ver comprometido los sistemas de redes, la confidencialidad de la información, los servicios y otras situaciones que puedan exponer a sanciones legales a la Institución.

Alcance:

Se aplica esta Política a uso, manejo, acceso a la información mediante dispositivos electrónicos (computadoras, tabletas o móviles) y mediante la red local (alámbrica o inalámbrica) de la Institución cuyo fin realizar negocios o brindar servicios de la Institución o de interactuar con redes internas y sistemas empresariales, sean propiedad o no la Institución.

Toda la comunidad universitaria (empleados, profesores, estudiantes, consultores) tendrán la responsabilidad en su conciencia actuar con juicio responsable en el manejo responsable de los datos informáticos según las Políticas establecidas, así como las leyes y regulaciones que sean aplicables.

Es por ello que, esta Política se aplica a todos los empleados, contratistas, consultores, profesores, estudiantes y otros trabajadores en la Institución, ya sea remoto o presencial.

Política:

Uso General:

1) El personal de Sistemas de Información es(son) la(s) persona(s) responsable(s) en tomar acciones preventivas necesarias para proteger la confidencialidad de la información y su confiabilidad en datos contenidos en las distintas plataformas (locales o en la nube). Toda información, entrada de datos, materiales didácticos que hayan sido desarrollado con equipos Institucionales, y dentro de la jornada laboral de cada empleado (incluyendo contratistas y facultativos), es propiedad de la Institución.

2) Todo el personal de la Oficina o Departamento de Sistemas de Información de la Institución es plenamente responsable de:

    a. Establecimiento de normas aplicables en la asignación de cuentas de acceso, y la seguridad que aplica como lo es: contraseñas, control de acceso al "data center", la honradez, seguridad en la información y comunicaciones intranet como por Internet que sean enviados.
    b. Confirmar que toda información esté debidamente protegida de ataques cibernéticos o acceso no autorizado, mediante programas actualizados y subscripciones vigentes de Antivirus y equipos de "Firewall" para protección de accesos externos no autorizados.
    c. Monitorear toda actividad y conexión a Internet para que sea llevada a cabo conforme a esta Política de Seguridad Cibernética, y corroborar el buen funcionamiento de ésta.

3) El personal de Sistemas de Información debe revisar y actualizar la política periódicamente, y dar a conocer los cambios realizados a toda la comunidad universitaria.

4) Además, debe desarrollar un plan, implementar y ejecutar periódicamente auditorías para evaluar el cumplimiento a esta Política sea efectivo.

5) Toda violación a esta política puede conllevar sanciones, desde la revocación a cualquier privilegio de acceso a los Sistemas Informáticos y debe ser notificado al Presidente de la Institución.

Propiedad:

1) Todo equipo, redes de comunicación (alambrado o inalámbrico), servicios a plataformas (Moodle, JKG Systems, Office 365, Destiny Library Manager, Infotrac), documentos creados dentro de la Institución son propiedad de la misma y son para ser utilizados exclusivamente para los propósitos de los intereses de Humacao Community College. Se prohíbe el uso de los mismos para propósitos personales, envío de recreo personal o para manejo de asuntos privados ajenos a sus funciones en la Institución.

2) Está totalmente prohibido la reproducción, publicación, de toda información y contenido electrónico que se cree, genere o modifique mediante el uso de los sistemas de información de la Institución. Esto incluye: comunicación electrónica, datos o información obtenida a través de Internet o que se encuentre almacenada o contenida en las computadoras (estaciones de trabajo, tabletas y/o servidores), le pertenecerán en todo momento a la Institución, aunque haya sido

esfuerzo personal del usuario. Todo lo que sea para fines ajenos de la Institución está estrictamente prohibido. Por otra parte, no se permite emitir o compartir información sin la debida autorización por parte de la Oficina de Presidencia. Cualquier alteración a cualquier archivo en formato electrónico conllevaría sanciones disciplinarias.

3) Es deber de todo empleado, contratista, consultor o terceros, que trabaje para la Institución, reportar de inmediato el robo, pérdida o divulgación no autorizada de información propietaria de la Institución.

4) La responsabilidad de ejercer un buen juicio sobre el uso de los sistemas de información y la data contenidas en estos es de todos los componentes integrales de la comunidad universitaria. Si se tiene alguna duda sobre el uso adecuado de los sistemas informáticos, se debe consultar con su supervisor inmediato o con los asesores de la Institución.

5) Contenidos de correo electrónicos, la Institución no los controlará ni se editarán, a menos que sea requerido o necesario en conformidad a alguna disposición legal, procesos legales en curso o simplemente para proteger la integridad del servicio.

6) El servicio de correo electrónico institucional no se utilizará en ninguna circunstancia para propósitos ilegítimos.

Seguridad:

1) Se requiere que todos aquellos dispositivos móviles (celulares, tabletas, laptops) y computadoras de escritorio deban cumplir con las políticas de acceso a la red local de la Institución.

2) Está estrictamente prohibido compartir contraseñas a otros usuarios o personas ajenas a la Institución. De igual manera darle acceso a otra persona, sea de manera deliberada o por descuido al no proteger las contraseñas asignadas.

3) Las computadoras deben tener activo el protector de pantalla de forma automática al minuto de inactividad de la computadora, y que se requiera contraseña para continuar utilizando el equipo. Por otro lado, si el usuario va a dejar desatendido el equipo debe bloquear su cuenta antes de abandonar el escritorio. En el caso de los estudiantes, si éstos accedieron a sus respectivas cuentas en diversas plataformas, deben cerrar la sesión activa.

4) Cuando un usuario (sea administrativo, facultativo o estudiante) debe tener extremo cuidado al acceder a un mensaje recibido por correo electrónico sospechoso. De igual manera, descargar algún archivo adjunto sospechoso o de remitente desconocido, ya que estos pueden contener un "malware".

Uso Inaceptable:

1. Toda actividad en el ciber espacio ilegal, dentro de la red local y con equipos de la Institución, está estrictamente prohibida, bajo las leyes federales y estatales aplicables a instituciones postsecundarias.

2. Lo que a continuación se enumera, entra en la categoría de uso inaceptable y compromete la integridad de los procesos de la Institución:

a. Toda diligencia o acciones del Sistema y de la Red: Las siguientes actividades están estrictamente prohibidas, sin excepción alguna:

1. Violar los derechos de cualquier persona, entidad, organización o corporación que estén protegidos bajo la ley de derechos de autor, patentes, secretos comerciales y cualquier derecho de propiedad intelectual, donde se incluye la distribución, instalación y uso de productos piratas donde se incluye programas y archivos de video y audio.

2. Todo programa y herramienta que se asocie a los sistemas de información de la Institución, deben contar con su correspondiente licencia vigente y autorizados para su uso. Estos programas y herramientas solamente debe ser instalado por el personal de la Oficina o Departamento de Sistemas de Información de la Institución o de Suplidores contratados. No se permite la instalación de programas sin la previa autorización de la Oficina o Departamento de Sistemas de Información, así sea libre de costo.

3. Queda prohibido hacer copias de cualquier "software" protegido por derechos de autor para el cual la Institución debe tener una licencia activa para su uso.

4. Acceder a datos, al servidor o a una cuenta para cualquier fin que no sea para fines corporativos de la Institución, incluso cuando el acceso esté autorizado.

5. La exportación de manera ilegal de "software", información técnica o tecnología de cifrado, en violación de las leyes sobre control de exportaciones.

6. Introducir programas maliciosos en la red o el servidor (por ejemplo, virus, gusanos, caballos de Troya, bombas de correo electrónico, etc.).

7. Revelar las contraseñas de acceso a otros o permitir el uso por terceros de una cuenta designada para uso exclusivo de una sola persona. Como regla general, está completamente prohibido compartir los accesos con terceros, bajo ningún concepto.

8. Utilizar recursos tecnológicos y computadoras de la Institución para participar activamente en la descarga, almacenamiento o envío de material que esté en violación de leyes sobre acoso sexual, pornografía, entre otras.

9. Causar brechas de seguridad o interrupciones en las redes de comunicación. Las brechas de seguridad incluyen acceder a datos de los cuales no es el destinatario o entrar en un servidor o en una cuenta a la que no se está expresamente autorizado.

10. Escanear puertos o escaneado de seguridad, a menos que se haga una notificación previa a la Institución.

11. Ejecutar cualquier forma de monitoreo de red que intercepte datos, a menos que esta actividad sea parte del trabajo o de las funciones del empleado.

12. Omitir la autenticación del usuario o la seguridad de cualquier "host", red o cuenta.

13. Utilizar cualquier programa ("script") comando, o enviar mensajes de cualquier tipo, con la intención de interferir o desactivar la sesión de un usuario, a través de cualquier medio, localmente o a través de Internet o Intranet.

b. Correos electrónicos y comunicación: Las siguientes actividades están estrictamente prohibidas, sin excepción alguna:

    1. El envío de mensajes por correo electrónico no solicitados, incluyendo el envío de "correo basura" o "junk mail" o cualquier otro material de publicidad a personas que no solicitaron específicamente dicho material ("email spam").

    2. Acoso por correo electrónico o llamada telefónica o mensajería de texto, ya sea por el lenguaje utilizado o la frecuencia de envío.

    3. Uso no autorizado, o falsificación de la información de encabezado del correo electrónico.

    4. Crear o reenviar "cadenas de mensajes" u otros esquemas de "pirámide" de cualquier tipo a través del correo electrónico.

c. Medios Sociales: Las siguientes actividades están estrictamente prohibidas, sin excepción alguna:
    1. La participación en medios sociales por parte de los empleados, aún cuando sea mediante el uso de computadoras, celulares o equipos personales, está sujeto a los términos y restricciones aquí establecidas. La participación debe darse de una manera profesional y responsable, y no podrá ser perjudicial para la Institución, esto no debe interferir con las responsabilidades y obligaciones del trabajo del empleado.

    2. No se permite bajo ningún concepto la divulgación de información confidencial de la Institución en ningún medio social.

    3. No se permite la participación a los empleados en ningún medio social que pueda dañar o empañar la imagen, reputación y/o buena voluntad de la Institución y/o cualquiera de sus empleados.

    4. Si el empleado expresa creencias y/u opiniones en medios sociales, éste no debe expresarse a nombre de la Institución.

    5. Todo logotipo de la propiedad intelectual de la Institución queda prohibido su uso en medios sociales sin la autorización de la Oficina de Presidencia.

d. Uso de Dispositivos de Almacenamiento o Medios Extraíbles:

    1. El uso de dispositivos de almacenamiento o medios extraíbles tales como; disco duro portátil, accesorios tipo USB, CD-R, CD-RW, DVD+R, DVD-R, DVD+RW o DVD-RW, o cualquier otro método de transferencia de información ya sea de manera física o electrónica a servidores en la nube ("cloud") o mediante el uso del correo electrónico, está totalmente prohibido a menos que sea propiamente autorizado.

2. Si el empleado necesita hacer uso de medios extraíbles, debe hacer la petición por escrito a la Oficina o Departamento de Sistemas de Información. Dicho medio extraíble de almacenamiento no debe salir de la Institución, a menos que sea autorizado por la Oficina de Presidencia.

3. La Oficina o Departamento de Sistemas de Información, en conjunto con la Oficina de Presidencia, serán los responsables de evaluar y aprobar la solicitud antes de que se pueda utilizar el dispositivo o medio solicitado. La aprobación de uso debe ser documentada por escrito y archivada para propósitos de auditoría.

Supervisión:

1. En cualquier momento la Institución podrá hacer auditorías, sin previo aviso, al correo electrónico, archivos personales, historial de navegación en la web y otra información guardada (almacenada) en los equipos tecnológicos de la Institución. Este ejercicio es para garantizar que se esté cumpliendo con la Política para el manejo de los sistemas de información de la Institución.

2. Esta supervisión se realizará de forma periódica, sin previo aviso, para prevención de ataques cibernéticos, uso incorrecto de equipos computadorizados Institucional, exposición a información confidencial de empleados y estudiantes. Las auditorías se podrán llevar a cabo por personal externo o interno de la Institución. Los resultados serán informados al Supervisor inmediato o al (la) Oficial de Recursos Humanos para su debido proceso correctivo o de amonestación.

3. La Institución se reserva la facultad de comenzar los procesos administrativos, civiles o criminales pertinentes a actos cometidos, aunque los mismos no estén incluidos expresamente en este documento, si los actos (directa o indirectamente), ponen en riesgo la seguridad, integridad y confiabilidad de la información y los sistemas de información de la Institución.

Jorge E. Mojica Rodríguez, Esq.
Presidente