POLÍTICA DE SEGURIDAD:

En la Universidad de Oriente nos preocupamos por la seguridad en el manejo de la información, por ello contamos con una política de seguridad, la cual se centra en los principios de:

● CONFIDENCIALIDAD: Proteger información valiosa y sensible de la divulgación no autorizada.

● INTEGRIDAD: Salvaguardar la exactitud e integridad de la información.

● DISPONIBILIDAD: Asegurar que la información y los servicios estén disponibles para los usuarios.

Esto implica que todas las entidades que interactúan interna y/o externamente con la Universidad, actuarán siempre acorde a la política de seguridad de la información establecida; y a su vez, realizar un seguimiento a las acciones que se realicen. Fomentando un manejo confidencial y responsable.

La política de seguridad se aplica bajo las siguientes consideraciones:

a) Estar disponible como información documentada

b) Ser comunicada dentro de la universidad

c) Estar disponible para las partes interesadas.

Para garantizar lo anterior, la Universidad refuerza la responsabilidad sobre las acciones realizadas dentro de los procesos operativos, funcionales y de resguardo de la información; así como el cuidado de los roles de ac ceso a la información, manteniendo el control de acceso a los activos de información, con base en los principios de “Necesidad de Saber” y “Necesidad de Hacer” acorde a los roles de trabajo.

Por ello establece las siguientes acciones: Los sistemas de información, los recursos tecnológicos, las bases de datos son accesibles únicamente por las personas autorizadas por la Universidad.

● Los responsables de los datos de las Universidades de Oriente, se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento durante su vigencia, así como la periodicidad con la que se cambian.

● A través del Departamento de Sistemas y Tecnología Integradas proporcionará al trabajador el equipo de cómputo en su espacio asignado para el desarrollo de sus actividades laborales, solo puede acceder a los sistemas, aplicaciones y servicios que le han sido aprobados.

● Utilizar un repositorio virtual para guardar la información, en caso de almacenarla en los discos locales del equipo asignado, se debe utilizar la partición protegida y descargar la información en los repositorios institucionales posteriormente, para prevenir que, ante una situación de hurto del equipo de cómputo, se pierda y exponga la información de la institución.

● El acceso a los sistemas de información se asigna de acuerdo a los perfiles autorizados para realizar las labores propias del cargo, así como el hardware y software otorgado, se utiliza únicamente para llevar a cabo las actividades laborales asignadas por el campus.

● Todo colaborador debe dar cumplimiento a la seguridad de la información asociados a la clasificación, etiquetado y manejo de documentos e información y bases de datos personales, considerando los criterios de confidencialidad de documentos.

● Todo usuario de la comunidad que posea una cuenta de correo institucional, puede acceder a esta dentro o fuera de las instalaciones de cada uno de los campus vía web.

● Los sistemas de información que almacenan, procesan o transmiten información clasificada como confidencial, en infraestructura tecnológica (Físicos o virtuales) o contratados a terceras partes (Físicos o en Internet), deberán asegurar la generación de copias de respaldo, su periodo de retención, rotación y métodos apropiados para su restauración.

● La administración de cuentas contempla los distintos tipos de cuenta y las medidas pertinentes para la vinculación o la desvinculación del personal directo o indirecto. Entre ellos se crea, cancela o deshabilita los permisos de acceso a los sistemas de información que el usuario utilice y se elimina cualquier vínculo a nivel de publicaciones y de cualquier tipo contractual que se encuentre habilitado.

● Es obligación del Departamento de Sistemas y Tecnología Integradas, garantizar el correcto funcionamiento de los equipos de cómputo, razón por la cual desde allí se concretan tiempos de mantenimiento de los equipos con los colaboradores. El mantenimiento se realiza de acuerdo con los procedimientos definidos en el marco del sistema de gestión de la calidad institucional.

Atentamente Comité de Seguridad de la Información.