UNIVERSIDAD CATÓLICA NORDESTANA

Seguridad de la Información

Seguridad de la Información.

Seguridad del Personal:

Todo usuario que tenga acceso a los sistemas y servicios informáticos debe firmar un convenio, en el que acepte las condiciones de confidencialidad, así como el uso adecuado de los recursos informáticos y de información de la UCNE.

Responsabilidades del Usuario:

El departamento de ITS entrega a cada empleado el nombre de usuario y la contraseña de equipo y acceso a la red, de la cual sólo él podrá hacer uso de la misma. Como norma general, los usuarios no podrán acceder a recursos para los que no estén debidamente autorizados.

Es un compromiso de todos los usuarios, cumplir las Políticas y Estándares de Seguridad en Informática establecidas por la Institución.

Políticas y Normas de Control:

Si el Departamento de ITS, identifica que hubo una violación a las políticas de seguridad de la información establecidas en la UCNE, procederá a enviar un reporte al departamento RRHH, para aplicar las sanciones establecidas en el reglamento interno de trabajo.

Se consideran violaciones graves, el copiar, almacenar, visualización no autorizada de archivos de los demás, robar, dañar y divulgar información reservada o confidencial de la UCNE, tales como: correo electrónico, fax, conversaciones telefónicas, documentos digitales e impresos.

La UCNE puede sancionar a los usuarios que quebranten las políticas de seguridad de la información, bloqueando su a la acceso a la red, como también puede ser sancionado, tanto dentro como fuera de la Institución. Este procedimiento puede llevarse a cabo cuando sea pertinente, con el fin de proteger la honestidad, seguridad y funcionalidad de la UCNE.

Cualquier persona que se entere del mal uso de la tecnología de información podrá notificarlo al Departamento de ITS.

Confidencialidad

La Universidad Católica Nordestana, UCNE, labora administrativamente en horarios diurnos, por lo cual un empleado no autorizado estará bloqueado a realizar ciertas tareas dependiendo de su perfil después de ciertas horas.

Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia.

Nuestros objetivos principales:

- **Integridad**: garantizar que la información de los estudiantes sean los correctos, por ejemplo: Dni, Datos Personales, Notas, ect.
- **Confidencialidad**: asegurar que sólo la o las personas autorizados tengan acceso a la información de los estudiantes, por ejemplo las notas, estado de normativa (financiero y académico) , solo varios departamentos dentro de la universidad pueden ver estos datos.
- **Disponibilidad**: garantizar que los sistemas de información (Contable y Académico) siempre estén disponible a la hora que un estudiante o padre necesite de ello.
- **Evitar el rechazo**: garantizar de que no pueda negar una operación realizada.
- **Autenticación**: asegurar que sólo los individuos autorizados tengan acceso a los recursos. Si alguien pierde la clave, debe solicitar por escrito explicando por qué no tiene el acceso al sistema y demostrar que es la persona que solicita la dueña de la información.

- Empleado de la universidad tienen un usuario asociado a su departamento vía perfiles, esto nos garantiza que no puedan entrar a módulos del sistema que no le corresponden.

- Profesores tienen clave y usuarios para entrar al portal de la universidad para visualizar sus estudiantes, las actas de notas por publicar y las no publicadas.

- Estudiantes por igual para ver su horario, notas publicadas, progreso académico, etc. Cada vez que alguien que tiene acceso se conecta al sistema y realiza una acción, el sistema registra y guarda el usuario, que hizo, la hora y fecha que entro, hasta la dirección IP desde donde lo realizo.

Medidas de Seguridad Implementadas para Asegurar los Sistemas:

- Para esto, se cumplen con los ***criterios de seguridad*** al uso para todo el software que se implante en los sistemas, partiendo de estándares y de personal suficientemente formado y sensibilizado con la seguridad. Esto se realiza a través de una base de datos de pruebas, así que, antes de aplicar cualquier mejora, actualización de software se implemente en ella y se realizan todas las pruebas pertinentes antes de ponerlo en ejecución en la base de datos real.

- ***Medidas de seguridad físicas (Infraestructura):*** sistemas anti incendios, vigilancia de los centros de proceso de datos, sistemas de protección contra inundaciones, protecciones eléctricas contra apagones y sobretensiones, sistemas de control de accesos, etc.

- Con respecto a las ***contraseñas,*** se les informa a las personas involucradas que están deben se difíciles de averiguar que, por ejemplo, no puedan ser deducidas a partir de los datos personales del individuo o por comparación con un diccionario, y que se cambien con la suficiente periodicidad.

- ***Vigilancia de red***. Las redes transportan toda la información, por lo que además de ser el medio habitual de acceso de los atacantes, también son un buen lugar para obtener la información sin tener que acceder a las fuentes de la misma.

- ***Medidas Protectoras:*** cortafuegos, sistemas de detección de intrusos (antispyware), antivirus, llaves para protección de software, etc.

- Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

- ***Copias de seguridad (Backup)*** e, incluso, sistemas de respaldo remoto que permiten mantener la información en dos ubicaciones de forma asíncrona.