Ministerio de Salud Pública

Plan de Seguridad Informática

Facultad de Enfermería
“Lidia Doce”

“La experiencia nos ha enseñado que aquello que no se controla con efectividad, no se cumple o se ejecuta superficialmente…. Se impone trabajar y preservar el orden, disciplina y exigencia”

Raúl Castro Ruz

El Plan de Seguridad Informática constituye el documento fundamental para el control y la seguridad en la explotación de las tecnologías informáticas de la Facultad.

Las medidas que se establecen en el presente Plan de Seguridad Informática son de obligatorio cumplimiento para todo el personal que haga uso de las tecnologías informáticas instaladas en la institución.

Políticas de Seguridad Informática de los usuarios que hacen uso de las tecnologías informáticas.

- Los usuarios que hagan uso de las tecnologías informáticas son responsables de la protección de la información que utilicen o creen en el transcurso del desarrollo de sus labores, lo cual incluye: protección de acceso a los locales y a sus microcomputadoras, así como cumplir con lo establecido respecto al tratamiento de la información oficial que se procese, intercambie, reproduzca o conserve a través de las tecnologías de información, según su categoría y demás regulaciones.
- Los usuarios tendrán acceso sólo a los recursos que necesitan en el cumplimiento de su labor diaria, implementándose mediante la definición del equipamiento, aplicaciones a utilizar mediante los privilegios y derechos de acceso a los activos de información que se le otorgue.
- Los jefes de áreas deben garantizar que la seguridad informática sea tratada como un problema institucional normal al ser afrontado y resuelto, siendo los máximos responsables de promover la seguridad informática en su área.
- Se emplearán las tecnologías informáticas y los servicios asociados con fines estrictamente de trabajo.
- Se realizarán salvas que permitan identificar y autenticar a los usuarios en correspondencia con el empleo a que están destinadas la información que en ellas se procese, intercambie y reproduzca.
- Todo software traído a la entidad se le aplicará un período de cuarentena que permitan asegurar su funcionamiento seguro. El Responsable de Seguridad Informática supervisará todo chequeo que se realice en aras de proteger la integridad de la información de que se dispone.
- Es obligatorio la desinfección de los dispositivos externos antes de su uso en las tecnologías informáticas.
- Se mantendrá actualizada la libreta de control de usuario. En el uso de las tecnologías informáticas de acuerdo a lo que se establece en el Reglamento de Seguridad para las Tecnologías de la Información emitido por el MIC.
- Los jefes de áreas y usuarios que hagan uso de las tecnologías informáticas las protegerán contra posibles hurtos, así como del robo de la información que contengan.

- El movimiento del equipamiento informático debe ser aprobado por el responsable de la seguridad informática, siguiendo los lineamientos establecidos por el sistema de medios básicos contable.
- Sólo podrá operar el servicio de correo electrónico el personal autorizado por la Decana.
- Los compañeros que no posean cuentas de correo y necesiten enviar y/o recibir mensajería electrónica deberán contar con la autorización de la Decana.
- En caso de recibirse ficheros anexos a los mensajes se tendrá en cuenta la revisión antivirus y el proceso de cuarentena de ser necesario.
- Sólo se accederá a los servicios de Internet desde las microcomputadoras autorizadas para ese fin.
- Aun cuando sea posible la conexión a un sitio de correo libre como Yahoo o Hotmail, los usuarios autorizados al uso de INTERNET se abstendrán de hacerlo, así como la difusión a través de las redes públicas de servicios de conversación en tiempo real (chat) por parte del personal de la entidad. Solo será autorizado en algunos casos por la dirección de la entidad en correspondencia a sus intereses y de las normas particulares establecidas para estos servicios y serán objetos de comprobación.
- Utilizar el correo electrónico e Internet según lo establecido en las normas vigentes (Código de Ética).

Sistema de Seguridad Informática

- Habilitar y llevar los registros que se indican en el sistema de medidas y aplicar los procedimientos que se incluyen como parte de este Plan de Seguridad Informática.
- Velar porque se apliquen los productos de protección de producción nacional u otros autorizados oficialmente para su uso en el país, debidamente actualizados.
- No transgredir ninguna de las medidas de seguridad establecidas.
- Cumplir las reglas establecidas para el empleo de las contraseñas.
- No introducir ni utilizar en las tecnologías ningún producto ni modificar la configuración de las mismas, sin la correspondiente autorización del responsable de seguridad informática.

Apertura y Cierre de los locales

El control de acceso y cierre de los locales está establecido que todas las áreas con tecnologías de información al terminar la jornada laboral queden cerradas y debidamente selladas, aquellas donde se maneje información clasificada los trabajadores de estas áreas deberán extremar las medidas de seguridad.

Al operar el equipamiento informático y en aras de su preservación se tendrá en cuenta:

- Apagarlos completamente antes de conectarlos o desconectarlos de la red eléctrica.
- Deberán quedar apagados al concluir la jornada laboral, salvo que por necesidades de explotación continua del sistema o de comunicaciones tengan que seguir funcionando.
- En caso de ocurrencia de tormentas eléctricas severas se apagarán y desconectarán todas las tecnologías informáticas y de comunicaciones, salvo aquellas que por necesidad imperiosa haya que dejar funcionando, en cuyo caso se crearán las condiciones necesarias para su protección.
- Se procederá a desconectar los equipos de la red eléctrica en caso de reparación o instalación eléctrica en la institución.
- En caso de fenómenos atmosféricos deberá desconectarse los equipos de la red eléctrica y de conexión.

- Mantener la limpieza de las microcomputadoras y sus accesorios; no limpiar con paños húmedos.

Control de Acceso a las Tecnologías Informáticas

- El Jefe de cada área determinará la manera en que utilizará el personal a él subordinado, las tecnologías informáticas, de forma tal que se logre un uso racional de las mismas.
- Los trabajadores que necesiten el uso de las tecnologías informáticas y que por razones objetivas no lo puedan hacer desde sus áreas correspondientes, deberán contar con la autorización de los Jefes de áreas y registrarse en la libreta de control de usuario del área en el que lo efectué.
- Para que una persona externa tenga acceso a las tecnologías informáticas y de comunicaciones será necesario la autorización previa de la decana y/o el responsable de seguridad informática y no se hará sin la presencia de un trabajador del área que se trate.

Identificación de usuarios

- Se establece identificación de usuarios en todas las microcomputadoras, así como para establecer la conexión a los servicios del correo electrónico e Internet.
- Cada área habilitará el uso del protector de pantalla con contraseña y el bloqueo de cuentas lo que evitará que la información sea vista en momentos de inactividad y la entrada de intrusos.
- Para el trabajo con los servicios de Correo electrónico e Internet, se tendrá en cuenta que no se realice la conexión automática a partir de las aplicaciones empleadas para su gestión.
- Se establecerá identificación de usuarios en las microcomputadoras de cada área en correspondencia al personal que haga uso de las tecnologías informáticas y comunicación.

Las contraseñas cumplirán los siguientes requisitos:

• Tendrán un período de vigencia con cuotas mínimas de 1 día y máximas de 90 días de duración, no obstante se permitirá cambiarlas fuera de estos términos de tiempo máximos y mínimos cuando las condiciones así lo exijan y lo cual será avalado por el Responsable de Seguridad Informática.
• Estas poseerán de permitirlo el equipo y/o sistema operativo, de 6 a 8 caracteres alfanuméricos como mínimo, no obvios, con al menos 1 de ellos de caracteres especiales y no se permitirá la duplicidad de las mismas.
• La contraseña cambiada con la periodicidad adecuada no se podrá repetir antes de que haya transcurrido un año como mínimo, desde que hubiera dejado de utilizarse.
• No utilizar contraseñas que sean palabras del diccionario (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
• No usar contraseñas completamente numéricas con algún significado (teléfono, C.I., fecha de nacimiento, Chapa del automóvil, etc.).
• No se compartirán entre usuarios que no sean del área.
• No contendrán patrones repetitivos como por ejemplo: Pazpazpepepepe.
• No contendrán secuencias de caracteres cercanos en el teclado, Ej. Asdfuio.
• Deben ser fáciles de recordar para no verse obligado a escribirlas.
• Nunca compartir con nadie la contraseña. Si se hace, cambiarla inmediatamente.
• No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.

- No teclear la contraseña si hay alguien mirando. Es una norma táctica de buen usuario no mirar el teclado mientras alguien teclea su contraseña.
- No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si se debe mencionar no hacerlo explícitamente diciendo: "mi clave es...".

En todos los casos los cambios de contraseñas deben informarse al Responsable de Seguridad Informática. Para ello, el usuario debe escribir la contraseña en un papel que se guardará en un sobre identificado con el nombre del área.

Prohibiciones

- Adición de algún equipo a la red, así como la instalación de cualquier tipo de software y de programas en las microcomputadoras sin la autorización del Responsable de Seguridad Informática, garantizando su compatibilización con las medidas de seguridad establecidas por MIC.
- La presencia de carpetas personales que contengan: programas de instalación, videos, películas, seriales y documentos que no estén en correspondencia con la actividad fundamental de la entidad así como música por más de 1GB de capacidad.
- La colocación de páginas o sitios Web desde entidades estatales en servidores extranjeros que ofrezcan estos sitios de manera gratuita.
- Vincular cuentas de correo electrónico de un servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través del mismo.
- Cualquier persona natural y jurídica a explotar o monitorear las redes públicas de trasmisión de datos en busca de vulnerabilidades o información sobre los usuarios legales de las mismas.
- Introducir, ejecutar, distribuir o conservar en los medios de cómputo programas que puedan ser utilizados para: comprobar, monitorear o transgredir la seguridad, así como información contraria al interés social, la moral y las buenas costumbres.

Cualquier problema que sea detectado por los jefes de áreas y usuarios que hagan uso de las tecnologías informáticas y comunicaciones en materia de seguridad informática deberán informar al responsable de seguridad informática de la institución, quien tratará de subsanar lo ocurrido e informará a la decana.

Osmany Alonso Ayala
Responsable de Seguridad Informática