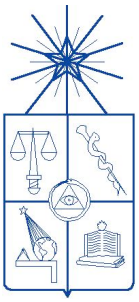
FACULTAD DE MEDICINA
UNIVERSIDAD DE CHILE



POLÍTICA DE INFRAESTRUCTURA INFORMÁTICA

INTRODUCCIÓN

La Facultad de Medicina de la Universidad de Chile reconoce como obligación contar con la seguridad apropiada para todos los datos, equipos y procesos informáticos y tecnológicos, que sean de su propiedad o que estén bajo su control.

El secreto de la información corresponde por mandato legal, por política universitaria, acuerdo explícito o convencional, según se trate.. Diversas clases de información autorizan diversos grados de secreto.

Los componentes del hardware y de software que constituyen la infraestructura de la Facultad, representan una inversión importante que debe ser protegida. Lo mismo ocurre con la información almacenada en los sistemas respectivos.

El uso de los activos de la Facultad en forma contraria al propósito con el cual fueron implementados representa un mal aprovechamiento de los recursos y eventualmente podría implicar una infracción legal.

Finalmente, la correcta funcionalidad de los sistemas informáticos es requerida para la operación eficiente y eficaz de la Facultad.

La política de redes e infraestructura informática, comprende los aspectos siguientes:

1.- Política de Seguridad Informática.
2.- Estándar para la utilización de infraestructura computacional y redes.
3.- Uso apropiado de Internet y correo electrónico.

1. POLÍTICA DE SEGURIDAD

Definición

La seguridad en informática es "el estado de estar libre de riesgo inaceptable". El riesgo se refiere a las siguientes categorías de pérdidas:

a. Secreto de la información: se refiere al resguardo de la información personal o corporativa incluyendo aplicaciones copyright.

b. Integridad de datos: La integridad se refiere a la exactitud de los datos. La pérdida de integridad de datos puede ser evidente como cuando un disco falla, o puede ser sutil, como cuando un carácter de un archivo de altera.

c. Activos: Los activos que deben ser protegidos incluyen:
   - Computador y equipo periférico.
   - Equipo y sistema de Comunicaciones.
   - Medios de almacenaje de las fuentes y de datos.
   - Programas y documentación del computador del sistema.
   - Programas y documentación del computador de uso personal.
   - Información.

d. Uso eficiente y apropiado de la información: se asegura de que los recursos de la Facultad de Medicina de la Universidad de Chile sean utilizados para los propósitos para los cuales fueron pensados.

e. Disponibilidad de sistema: se refiere a la funcionalidad completa de un sistema y de sus componentes.

Dominios de la seguridad

Esta política se ocupará de los siguientes ámbitos de seguridad:

- Seguridad del sistema informático: CPU, Periférico, Sistema Operativos. Esto incluye seguridad de datos.
- Seguridad física: Procedimientos del personal de Informática.
- Seguridad operacional: Control ambiental, equipo de energía, actividades de operación.
- Seguridad de usuarios.
- Seguridad de comunicaciones: Equipos de comunicaciones, personal, trayectorias de transmisión y áreas adyacentes.

Roles y Responsabilidades

La formulación de la política corresponde a las autoridades superiores de la Facultad y su puesta en marcha y manteniendo, son responsabilidad de la Dirección Económica y de Gestión Institucional a través de la Subdirección de Informática y Telecomunicaciones.

Implementación de la política

- Cada miembro de la Facultad es responsable de conocer y cumplir los estándares y políticas establecidos.
- La subdirección de Informática y Telecomunicaciones es responsable de velar y mantener las políticas operativas.

Custodios

- La subdirección de Informática es responsable de la seguridad de la infraestructura computacional estratégica de la Facultad.
- La seguridad de la infraestructura de oficinas, unidades administrativas y/o académicas, salas y laboratorios es de responsabilidad de cada jefatura.
- Los usuarios finales son responsables de la seguridad de los computadores asignados así como de los equipos personales.

Usuarios

Todas aquellas personas que utilizan recursos informáticos de la Facultad de Medicina de la Universidad de Chile:

- Deben operar bajo las "Condiciones de Uso" según los estándares y pautas para la utilización de recursos informáticos en la Facultad.
- Debe comportarse de acuerdo al "Código de buenas prácticas" explicitado más abajo y según los estándares y pautas para la utilización de recursos informáticos en la Facultad.
- Son responsables del apropiado uso y cuidado de los recursos informáticos bajo su control.
-

Servicios de la Facultad de Medicina de la Universidad de Chile

Se reconoce que varias unidades de la Facultad, proporcionan servicios que se relacionan con la seguridad informática directa o indirectamente. Se espera que exista colaboración entre estas unidades en la generación de las políticas de seguridad y su puesta en práctica.
Algunas de estas unidades son:

- Recursos Humanos: Selección, inducción, y proceso de desvinculación del personal.
- Secretarias: Políticas referentes a aislamiento del secreto, y copyright.
- Logística: Seguridad física del edificio, Sistemas de respaldo de energía.

2. ESTÁNDAR PARA LA UTILIZACIÓN DE INFRAESTRUCTURA COMPUTACIONAL Y REDES.

Condiciones para el uso de Infraestructura computacional.

1.- Es política de la Facultad, que la infraestructura computacional y de redes sean utilizadas exclusivamente para la docencia, aprendizaje, investigación y administración, de acuerdo a los objetivos y misión de la Facultad.; conforme al Código de Buenas Prácticas que se especifica más adelante.

2.- Toda persona que utilice la infraestructura computacional y de redes de la Facultad, será responsable de su utilización según se especifica en el Código de Buenas Prácticas y deberá respetar las condiciones y términos de uso especificadas por la administración de la Infraestructura.

3.- La infraestructura computacional y de redes no puede ser utilizada para fines comerciales o en actividades no relacionadas con la Facultad, a no ser que cuente con la respectiva autorización de la jefatura directa.

4.- El usuario no podrá registrar ni procesar información que infrinja cualquier patente o derecho de autor.

5.- La Facultad protegerá la confidencialidad de la información de los usuarios, pero no se hará responsable por el uso incorrecto de ésta..

6.- La Facultad resguardará la información respaldando a quien lo solicite dentro de los computadores y redes, pero no se hará responsable ante un evento de pérdida. El usuario deberá mantener un mínimo de medidas orientadas a resguardar su información contenida en los computadores y redes de la Facultad.

7.- Si existiere pérdida de información dentro de los sistemas, la Subdirección de Informática y Telecomunicaciones, hará lo posible por recuperar la información y apoyará al usuario en la recuperación de la falla.

8.- El uso de computadores y redes, es permitido por la Facultad con la condición de que esta no signifique infracción de las leyes vigentes, entre éstas la de patentes y de propiedad intelectual

9.- Cuando los usuarios de la infraestructura computacional de la Facultad piedan su calidad de tales por dejar de ser académicos, funcionarios o estudiantes,

su información será eliminada de los sistemas y computadores, sin ningún tipo de notificación. Oportunamente, los usuarios deberán eliminar su información o acordar de antemano el respaldo de ella.

10.- La Facultad se reserva el derecho a limitar cualquier uso de infraestructura computacional y hacer esto sin previo aviso con tal de proteger la integridad de la infraestructura, computadores y redes de un uso no autorizado o inadecuado y resguardar así su funcionalidad para el resto de los usuarios.

11.- La Facultad, a través de personal autorizado, se reserva el derecho de revisar y monitorear periódicamente los computadores y redes, y se reserva cualquier otro derecho necesario para su protección.

12.- La Facultad no se hace responsable por pérdida o destrucción de información de usuarios como resultado de acciones necesarias para mantener la privacidad, seguridad e integridad de la infraestructura computacional.

13.- La Facultad se reserva el derecho de tomar acciones de emergencia para resguardar la integridad y seguridad de la infraestructura informática. Esto incluye finalizar programas o procesos que están operando o alterar temporalmente, cuentas y password de usuarios,

14.- Los usuarios de la infraestructura computacional, operarán bajos las normas y políticas de la Facultad y leyes del país. La Facultad no se responsabilizará ni garantizará la información ni materiales ubicados en los sistemas que no son de la Facultad o que están disponibles públicamente, excepto donde la responsabilidad se exprese formalmente. Tal material e información no reflejará necesariamente las actitudes y opiniones o los valores de la Facultad, de su personal o estudiantes.

15.- El Subdirector de Informática y Telecomunicaciones solicitará investigación sumaria o sumario administrativo en el caso de: daño intencional de la infraestructura informática; constatar obtención de información confidencial de manera impropia; destrucción de información; interrupción en forma intencional del servicio; infringir cualquier patente o propiedad intelectual; obtener o intentar obtener accesos no autorizados a cuentas y password.

Código de Buenas Prácticas en el uso de computadores y red de datos

Corresponde al uso apropiado y responsable de la infraestructura computacional de la Facultad. Se define como el uso orientado a la docencia, investigación, extensión y los objetivos administrativos de la Facultad para los cuales su uso fue autorizado. Toda utilización contraria a estos objetivos se considera como uso inadecuado.

Se entiende que los usuarios de la infraestructura computacional de la Facultad aceptan desde ya las siguientes responsabilidades:

1.- Seguridad, que implica:

- Resguardar sus datos, información personal, passwords y datos confidenciales.
- Utilizar los mecanismos de seguridad de los computadores.
- Elegir sus passwords cuidadosamente y mantenerlas a resguardo.
- Seguir las políticas y procedimientos de seguridad de control de accesos.

2.- Confidencialidad, que implica:

- Respetar la privacidad de otro usuarios;
- No hacerse pasar por otro usuario,
- No divulgar información personal sin autorización.

3.- Respetar los derechos de otros usuarios.

4- Respetar las protecciones legales de licenciamiento y propiedad intelectual.

5.- Respetar la integridad de la infraestructura computacional.

6.- Adherir a todas las políticas y procedimientos de la Facultad que incluyen políticas de un apropiado uso de los recursos e infraestructura computacional; la adquisición, uso y disposición de equipo computacional; uso de equipo de comunicaciones; uso de software legal; y uso legal de datos administrativos.

Buenas Prácticas en Actividades Específicas

Lo que aplica a las siguientes actividades específicas:

1.- Actividad Ilegal.
En general, es ilegal el inapropiado uso, almacenamiento o acceso a información o utilización de la infraestructura de la Facultad que pueda resultar en acciones legales contra la propia Facultad o Universidad.

2.- Material No Adecuado.
La infraestructura computacional de la Facultad no debe ser utilizada en la transmisión, obtención, demostración, almacenamiento de material no adecuado tal como:

- Material clasificado (con publicación prohibida)
- Pornografía.
- Pornografía infantil.
- Artículos que promuevan el crimen, discriminación o violencia.

3.- Software y Hardware Restringido.
Los usuarios de la infraestructura computacional no pueden instalar, bajo su conocimiento, ni autorizar la instalación o ejecutar programas que violen las políticas de seguridad y licencias de la Facultad y Universidad. No se puede ejecutar ni instalar programas tales como virus, troyanos, gusanos, detectores de password y analizadores de tráfico. Es necesaria la autorización de la Subdirección de Informática y Telecomunicaciones si alguno de estos programas es requerido para investigación.

4.- Desarrollo de Negocios Personales.
La infraestructura computacional no puede usarse en negocios personales que no estén relacionados con la Facultad de Medicina.

5.- Interconexión a las Redes de Datos de la Facultad.
Es responsabilidad de la Subdirección de Informática y Telecomunicaciones velar por la integridad de la infraestructura computacional y sus redes, por lo cual su mantención sólo puede ser hecha por personal especializado bajo la supervisión de esta Subdirección. Todos los requerimientos de nuevas conexiones de redes deben ser dirigidos a la unidad de Redes y Telecomunicaciones de la Subdirección de Informática.

No está autorizada la instalación de dispositivos de comunicación en la red de datos de la Facultad de Medicina si esta instalación no ha sido evaluada, autorizada, ejecutada y controlada por la Subdirección de Informática y Telecomunicaciones. Esta medida se debe a que se vulnera la seguridad de la red y degrada el rendimiento de las conexiones afectando a toda la comunidad universitaria.

3. USO APROPIADO DE INTERNET Y CORREO ELECTRÓNICO

A. Internet.

Transmisión de la Información

1.- Descarga (Download).
Todo programa (software) descargado vía Internet debe ser limpiado de virus antes de su ejecución. La Subdirección de Informática y Telecomunicaciones provee de la instalación de un antivirus para todos los equipos de la Facultad y es responsabilidad del usuario solicitar dicha instalación y mantener el antivirus actualizado y operativo.

2.- Información No Validada.
Toda información extraída de Internet debe ser considerada como no validada (no oficial) hasta que sea comparada y confirmada con fuentes oficiales.

3.- Contactos.
Contactos hechos a través de Internet que no estén validados por la Facultad (o la Universidad) deben ser validados y legitimados.

Seguridad Personal

1.- Privacidad.
Académicos, estudiantes y funcionarios que utilizan los sistemas de información y/o Internet deben reportar que los datos no son automáticamente protegidos de terceras partes.

2.- Derecho de Examinar y Auditar.
En cualquier tiempo y sin previo aviso, administradores de la Facultad y Universidad y, bajo la autorización de las respectivas jefaturas y autoridades, se reserva el derecho de examinar el correo electrónico, directorios y carpetas de archivos personales y en general cualquier información almacenada en los computadores de la Facultad. Este examen puede hacerse con los propósitos de asegurar las políticas de seguridad, permitir la continuidad de las funciones de administración, docencia o investigación, o asistir en la administración de los sistemas de información.

3.- Utilización de los Recursos.
La Facultad permite que el personal de colaboración navegue en Internet, pero si esta navegación es para propósitos personales debe realizarse fuera del horario de trabajo.

4.- Representación Pública.
Académicos y Personal de Colaboración pueden indicar su afiliación con la Facultad en boletines de discusión u otro tipo de grupo en Internet dejando en claro que los comentarios expuestos no necesariamente representan el pensamiento de las autoridades de la Facultad. Una representación externa debe ser en acuerdo y con autorización de las respectivas autoridades de la Facultad.

Se debe tener especial cuidado en los comentarios y respuestas puestos en listas de correos, noticias públicas o cualquier medio de publicación en Internet, los que deben seguir las políticas comunicacionales de la Facultad y que son indicadas por la Subdirección de Comunicaciones.

Control de Acceso de las Redes

A no ser que se tenga autorización de la Subdirección de Informática y Telecomunicaciones, académicos, estudiantes ni personal de colaboración pueden instalar dispositivos de comunicación y establecer comunicación con redes externas que permitan acceso a las redes de la Facultad a usuarios ajenos a ella.

Reportes de Problemas de Seguridad

La Subdirección de Informática y Telecomunicaciones debe ser notificada inmediatamente cuando:

1.- Información de importancia para la Facultad esté siendo borrada o enviada a destinatarios no autorizados o existe sospecha de que esto ocurre.

2.- Exista uso no autorizado de los sistemas de Información o se sospeche de ello.

3.- Password sean pérdidas, mal utilizados o se sospeche de esto.

4.- Ocurran eventos inusuales tales como pérdidas de archivos, frecuentes caídas de sistemas, mensajes extraños.

B. Correo electrónico

El correo electrónico es un servicio facilitado por la Facultad para su uso en la docencia, investigación, extensión y procesos administrativos. Su uso se rige por las reglas y políticas de la Facultad, Universidad y las leyes del Estado.

El correo electrónico puede ser utilizado para comunicaciones personales pero con uso apropiadamente limitado.

Los usuarios son responsables de asegurar que sus mensajes:

- No contengan información que dañen a la Facultad o miembros de la comunidad universitaria.
- Deben ser consistentes con las políticas de la Facultad.
- Proteger los derechos de privacidad y confidencialidad.
- No contener material obsceno ni ofensivo.
- No ser utilizado para propósitos que entran en conflictos con los intereses de la Facultad.
- Contener la apropiada firma.
- No sobrecargar de mail (No hacer Spam)
- No debe utilizarse para propósitos comerciales a no ser que esté autorizado.

Los correos electrónicos que contienen formales aprobaciones, autorizaciones, delegaciones u otros, podrán ser impresos para propósitos de control y auditoría.

Respaldo

Es responsabilidad de cada usuario respaldar sus datos y correos electrónicos.

Confidencialidad y Seguridad

1. El correo electrónico es de por sí inseguro ya que es una herramienta de uso generalizado en la actualidad y su funcionamiento ha quedado normado por estándares que facilitan la interacción, sin embargo tan solo contemplan elementos básicos de privacidad y ninguno de protección contra posibles intercepciones.

2. La comunicación vía correo electrónico se basa en que su transferencia es entre distintos servidores, internos y externos, nacionales e internacionales. Cada uno de estos servidores cuenta con mecanismos de seguridad tales como *antispam* o antivirus, por lo que, eventualmente, un correo podría no llegar al destinatario.

3. En el caso de funciones operativas donde el correo electrónico es parte de un flujo administrativo o académico, la jefatura o autoridad correspondiente podrá solicitar copia del correo entrante de un determinado funcionario que por algún motivo no se encuentre en sus labores (enfermedad, viaje, etc.) con fin de velar por la continuidad de las funciones operativas de la unidad.

4. En virtud del punto anterior, se recomienda que material personal o confidencial no sea almacenado o enviado a través de la infraestructura de la Facultad.

5. Usuarios deben asegurar la integridad de su password.

Responsabilidad

La Facultad no se hace responsable y no garantiza la entrega de cualquier archivo, mensaje o dato por el uso del correo electrónico.

Spam

El SPAM está definido como el envío de emails no solicitados. El email es uno de los principales medios de comunicación de Internet. Esta vía de contacto está siendo cada vez más degradada por el elevado número de correos de publicidad, información y/o divulgación de datos que llegan a los destinatarios sin haber sido solicitados por ellos. Esto se traduce en un elevado uso del espacio para el almacenamiento de mensajes, sobrecarga de los servidores que administran y trasmiten los emails, sobrecarga de las redes de comunicación, etc. Siendo así, todos los usuarios de la Facultad se responsabilizan por el uso de sus respectivas cuentas de correo y de no realizar SPAM bajo ningún pretexto. De lo contrario, se aplicará la política anti-spam correspondiente.

Por lo anterior:
1. La Facultad se reserva el derecho de suspender la cuenta por tiempo indeterminado al recibir alguna denuncia de Spam y comprobar el hecho, sin mediar aviso previo.

2. El envío de correo no solicitado, propaganda o divulgación masiva de información que afecte el correcto funcionamiento de los servidores por parte de un usuario de la Facultad, resultará en la inmediata suspensión de la cuenta pudiendo incluso llegar a cancelar la misma.

3. Esta prohibido enviar correo no solicitado utilizando el servidor saliente (SMTP) de la Facultad o desde un servicio de webmail, como por ejemplo yahoo o hotmail,

ya que también es considerado SPAM, y nuestros servidores pueden verse afectados en forma directa.

Política de correos masivos: Alternativas viables de comunicación interna.

Como es palpable por la comunidad, la proliferación de mensajes dirigidos a destinatarios colectivos con variados temas de la Facultad, poco a poco ha desnaturalizado su objetivo y distorsionado su función. El correo masivo ha perdido su objetivo de entregar información atingente a los públicos interesados en ella y su tráfico indiscriminado provoca dificultades en los servidores de la Facultad.

La Facultad de Medicina cuenta desde la aprobación de este documento con herramientas que permiten normar el uso del correo masivo como instrumento de comunicación interna. Así, los interesados en difundir información relevante por esta vía cuentan con listas segmentadas de direcciones electrónicas, esto es, grupos de destinatarios acordes con el tenor del mensaje.

Uso de contraseñas

- Las contraseñas deben ser memorizadas.
- Las contraseñas son individuales y no deben compartirse.
- Las contraseñas deben ser cambiadas inmediatamente si estas están comprometidas.

Resguardo legal

Violaciones de las políticas de seguridad indicadas en este documento pueden conducir a la restricción y/o suspensión de los privilegios de utilización de la infraestructura computacional de la Facultad sin perjuicio de los posteriores procedimientos administrativos y legales.

FACULTAD DE MEDICINA

UNIVERSIDAD DE CHILE