



UNIVERSIDAD
CAECE
SEDE MAR DEL PLATA

NORMAS DE USO DE LOS RECURSOS INFORMÁTICOS

Reglamento para el Personal Docente

1) EL REGLAMENTO

El presente reglamento dispone normas de uso y conductas que se aplican al uso de los recursos informáticos de la Universidad CAECE, sede Mar del Plata. Es responsabilidad del área de Sistemas y Tecnología velar por el cumplimiento de la siguiente normativa cuyo propósito es:

- Asegurar que los recursos informáticos se utilicen con los fines que se establecen en este reglamento,
- Evitar situaciones que pueden causar a la Universidad o a sus miembros algún tipo de responsabilidad administrativa, civil o penal,
- Proteger el prestigio y buen nombre de la Universidad y de sus miembros,
- Velar por la seguridad de los sistemas, optimizar el rendimiento de los equipos y salvaguardar la privacidad de los datos,
- Proteger los bienes y el esfuerzo realizado en la relación a la inversión tecnológica de abusos y usos indebidos que puedan mermar la disponibilidad o adecuación de los recursos, facilitar la labor del Área de Sistemas y Tecnologías en el cumplimiento de sus funciones.

2) USUARIOS DE LOS RECURSOS Y SERVICIOS INFORMÁTICOS

Se considera usuario de los recursos y servicios informáticos a todos los miembros de nuestra comunidad educativa, esto es, docentes, estudiantes, graduados, personal administrativo y de gestión, y a invitados o terceros autorizados, denominados todos ellos, en adelante, Usuarios, quienes deben avenirse al presente reglamento.

Los usuarios de recursos informáticos están obligados a aceptar la presente normativa desde el momento en que hacen uso de los recursos o servicios informáticos ofrecidos por la Universidad. Una copia de esta normativa debe estar siempre a disposición de los usuarios y publicada en el sitio Web de la Universidad.

El desconocimiento de esta normativa no exime de su cumplimiento. La Universidad se reserva el derecho de iniciar acciones oportunas en los casos previstos en esta normativa o contemplados directa o indirectamente en toda otra norma vigente de la Universidad, en especial en el Reglamento de Disciplina y Código de Ética (R.R. Nº 113/09) o de ámbitos mayores que le atañan, relacionadas con la protección de datos personales, la confidencialidad de la información, el uso del correo electrónico, el uso de Internet, etc.

3) LOS RECURSOS INFORMÁTICOS

Se considera bajo la expresión recurso informático a todos los dispositivos de procesamiento electrónico de datos, sistemas de información y comunicación, ya sean personales o compartidos, que sean administrados por la Universidad, estén o no conectados a una red institucional y a todos los servicios de comunicación y de procesamiento de datos.

Esta definición abarca al hardware, al software y al firmware de todos los equipos. Es decir, se incluye tanto a las computadoras de tipo servidor, personales o portátiles, a sus dispositivos periféricos, equipos de proyección, duplicación, sonido, video o fotográficos, dispositivos de comunicación, codificación y transferencia remota o local de datos y redes internas (intranets) o externas como a los programas, sistemas, bases de datos y archivos de datos en general.

Se extiende esta definición, además, a los ámbitos físicos destinados al uso de dispositivos de procesamiento electrónico de datos y a los ámbitos virtuales que soporten a los sistemas de información y comunicación.

En consecuencia, forman parte de los recursos informáticos tanto los laboratorios y ámbitos de estudio informatizados como el Campus Virtual, los sitios Web institucionales, los Sistemas de Autogestión y toda otra manifestación que materialice la comunidad virtual de la universidad o los servicios vía Internet que la Universidad preste a los Usuarios. El servicio telefónico de comunicaciones, incluidos teléfonos para comunicación con el exterior e internos también está incluido bajo este concepto y es abarcado por la presente normativa, al igual que todos los servicios virtuales, incluyendo al correo electrónico, FTP, conexión a Internet alámbrica e inalámbrica, etc.

3.1 Fines del uso de los recursos informáticos

Los recursos informáticos están destinados al uso académico, científico, de comunicación y de gestión relacionado con las actividades que se desarrollan en la Universidad.

3.2 Distinción de recursos académicos y administrativos

Los recursos informáticos están clasificados como recursos académicos y recursos administrativos. Los primeros están disponibles para alumnos, graduados, docentes, disertantes o terceros autorizados que realicen actividades académicas de cualquier índole. Los recursos administrativos, por su parte, están puestos a disposición de coordinadores académicos -en el cumplimiento de sus actividades de gestión-, personal administrativo, personal de gestión y terceros autorizados expresamente.

Los equipos administrativos pueden funcionar como servidores (de programas, de datos, de dominios, de impresión, de backup, de correo electrónico, de FTP, etc.) o como computadoras personales asignadas a un área o persona. No implica, este último caso, que las computadoras sean de uso exclusivo o privado de los Usuarios.

El área de Sistemas y Tecnologías puede reasignar recursos o asignar horarios de uso a distintos usuarios de acuerdo con las necesidades de la Institución.

No está permitido hacer uso de equipos administrativos con fines académicos ni viceversa sin la intervención del Área de Sistemas y Tecnologías.

3.3 Limitaciones en el uso de recursos informáticos y de telecomunicaciones

No está permitido el uso de los equipos y de la red informática y de telecomunicaciones para la realización de actividades ajenas a la Universidad de tipo comercial, que sean contradictorias con las normas de convivencia o con el espíritu de la Institución.

Los espacios y herramientas de comunicación (páginas o formularios Web, foros de discusión, blogs, correo electrónico, Chat, carteleras virtuales, etc.) que el área de Sistemas y Tecnologías ponga a disposición de los Usuarios, independientemente del tipo de interacción que se realice, son ámbitos virtuales de la Universidad. En consecuencia, los usuarios deben asumir una participación basada en la educación y el respeto al resto de los miembros de la comunidad educativa.

Se aplican en las aulas y espacios virtuales todas las reglamentaciones vigentes en la Universidad o el espíritu de las mismas, en caso de que no se adapten directamente. Asimismo, está prohibido desarrollar actividades encaminadas a romper la seguridad de los sistemas informáticos, así como sustraer o dañar el material o información existente.

Se mencionan expresamente como acciones que incumplen con esta normativa:

-La exposición o comunicación de contenidos o acciones, independientemente del medio con que se presenten y del recurso informático que utilicen, dirigidos o que pueden dar origen a producir algún tipo de interferencia o interrupción del funcionamiento de algún recurso informático de la Universidad o de cualquiera de los servicios ofrecidos o de terceros, así como actividades de "hackeo", "crackeo", "phreaking", o cualquier otra forma de intrusión, dentro o hacia fuera de la Institución.

-La búsqueda o rastreo de claves de acceso, direcciones IP, bugs o de puertas traseras (backdoors) de los sistemas de seguridad, etc. la captura de información que viaja sobre una red (sniffeeo) desde dentro o fuera de la red institucional y el uso de los sistemas para atacar, explorar o hacer "phishing" en cualquier sistema informático.

-La introducción intencionada de cualquier tipo de malware o spyware, ya sea que se trate de virus, troyanos, gusanos, etc. que puedan ser intrusivos, perjudiciales o nocivos para los sistemas informáticos de la Universidad y la ejecución de aplicaciones o rutina orientada a la destrucción, el deterioro o la obtención de información no autorizada que conlleven alguna responsabilidad civil o penal, o que pudiera violar cualquier ley local, nacional o internacional.

-La exposición o comunicación de contenidos o acciones, independientemente del medio con que se presenten y del recurso informático que utilicen, que puedan ser cuestionables u ofensivos. Queda, en ese sentido, terminantemente prohibido la exposición, comunicación o transferencia de cualquier material que pueda ser considerado ilegal, amenazante, dañino, abusivo, molesto, malicioso, difamatorio, calumniantes, de mal gusto, vulgar, obsceno, ofensivo, inaceptable, discriminatorio o pornográfico.

-La destrucción, sustracción o traslado no autorizado a otras dependencias de cualquier dispositivo físico de la infraestructura informática.

-La violación de los demás restricciones establecidas en la presente normativa.

3.4 Deberes de los usuarios respecto de los equipos informáticos

- Son deberes de los usuarios de recursos informáticos:
 - Contribuir al cuidado y conservación de las instalaciones, sistemas y equipos. Los usuarios deberán tener máximo cuidado en la manipulación y uso de equipos e infraestructura tecnológica, evitando cualquier acción que de forma voluntaria pueda dañar su integridad.
 - Contribuir al mantenimiento del orden en los laboratorios y demás espacios educativos. No fumar ni consumir ningún tipo de alimento o bebida, así como no hacer uso de teléfonos móviles en los ámbitos educativos.
 - Dejar los equipos en condiciones, bien apagados, correctamente conectados y en su lugar.
 - Facilitar la actividad de vigilancia y supervisión de los responsables de los recursos, poniendo a su disposición los equipos e identificándose si así fuera requerido.
 - Respetar las indicaciones que reciban de los responsables del mantenimiento de los sistemas informáticos respecto al funcionamiento y normas de uso de los laboratorios, equipos y sistemas.
 - Notificar al área de Sistemas las anomalías que detecten en los equipos, tanto de hardware como de software.
 - Hacer un uso adecuado y racional de los recursos informáticos. El usuario debe procurarse los conocimientos imprescindibles para el manejo de los dispositivos físicos y de los programas que necesite (con excepción de aquellos que constituyan objeto de aprendizaje por parte de los alumnos, en el momento en que estén asistiendo a las clases en que se enseñen dichos programas).
 - El cumplimiento de los demás requisitos y condiciones establecidos en la presente normativa.

4) SEGURIDAD EN EL ACCESO

El acceso a los recursos que requieran autenticación (red de datos, campus virtual, blogs, servicio de autogestión, correo electrónico, sistema telefónico, etc.) debe realizarse mediante una computadora personal conectada a Internet, mediante un dispositivo electrónico de comunicación o por cualquier medio lícito, proporcionando la información de acceso (nombre y contraseña) que se le suministre.

La información de acceso a los recursos que requieran autenticación es personal e intransferible de cada usuario. Por lo tanto, las actuaciones realizadas bajo una determinada contraseña e información de acceso se considerarán efectuadas por su titular quien debe custodiar la confidencialidad de esa información y no divulgarla a terceros, liberando a la Universidad de toda responsabilidad que de la divulgación intencional o no deliberada se derive.

Cada usuario debe velar para impedir el eventual acceso al recurso de ingreso restringido de

otros usuarios o personas ajenas a la Universidad con su propia información.

Un usuario tampoco puede interferir o intentar interferir la información que pertenece a otro usuario. Se menciona expresamente como acción que incumple con esta normativa a todo acto de ingeniería social tendiente a conseguir la información confidencial del propio usuario mediante engaños o manipulación.

Las claves de acceso deben ser modificadas por el usuario en su primer ingreso a aquellos servicio en los que esta opción esté disponible y, luego, con cierta frecuencia; en particular, si se presume el conocimiento de la misma por parte de terceros.

En el caso de servicios que no permitan al usuario modificar por sí mismo la clave de acceso, podrá solicitar al Área de Sistemas y Tecnologías su modificación, quien, asimismo, se reserva el derecho de blanquear las claves existentes y de asignar nuevos valores toda vez que, por cuestiones de seguridad o mantenimiento, lo considere pertinente.

4.1 Recomendaciones para las claves de acceso

A fin de garantizar la seguridad en el acceso a los recursos que requieren autenticación de usuario se recomienda utilizar claves de acceso con las siguientes características:

- Que sean únicas, es decir que no sean usadas en más de un medio virtual
- Que sean fáciles de recordar por uno pero difíciles de suponer o deducir por terceros
- Que tengan más de 6 caracteres, preferentemente alfanuméricos, siempre y cuando el recurso informático lo soporte.

Así mismo, se sugiere no utilizar claves de acceso con las particularidades que se mencionan a continuación:

- Que tengan 3 o más dígitos o caracteres iguales, sin importar su posición (por ejemplo, "1311" o "analia")
- Que sean números con dígitos correlativos ascendentes o descendentes (por ejemplo, "123456", o "987654")
- Que coincidan con otros datos personales tales como últimos o primeros dígitos del documento, el número de teléfono, fechas de cumpleaños, nombres de seres queridos, etc.
- Que Incluyan un año reciente (los números comienzan con 19... o con 20...)

Se recomienda expresamente no guardar la clave en la PC, en el mail o anotada en papel.

5) CONFIDENCIALIDAD DE LA INFORMACIÓN

Los usuarios deben respetar los datos considerados confidenciales o de uso restringido, a los cuales puedan, eventualmente, tener acceso en función de su condición de usuario recursos informáticos, de acuerdo con la Ley 25.326 de Protección de Datos Personales y normativa general vigente y aplicable.

Deben tener especial cuidado en no acceder a datos a los cuales no esté previsto o no se supon-

ga su acceso. Estos actos son ilegales aunque sólo sean con el propósito de ojear (browsing), curiosear (snooping), hacer descubrimiento electrónico (electronic discovery) o realizar exploraciones (exploiting).

Los usuarios no están autorizados a divulgar ni transferir a terceros la información a la que tengan accesos como consecuencia del uso de sistemas informáticos o documentales de la universidad ni a incorporarla a redes locales, nacionales o internacionales de transmisión de datos sin la autorización previa y expresa.

En particular, no pueden facilitar listados, copia de todo o parte de los documentos y/o datos personales de los alumnos ni de los trabajadores a los que pudiera tener acceso. Cualquier entrega de información a una persona o entidad externa a la Universidad no prevista y documentada en los procedimientos habituales requiere expresa autorización escrita de las autoridades de la Universidad.

Esta restricción se aplica expresamente a los datos de acceso a Internet, al campus virtual, a los servicios de autogestión u otros ámbitos Web restringidos, al uso del teléfono, del correo electrónico, de la Intranet, etc.

Se mencionan expresamente como acciones que incumplen con esta normativa a la alteración de la integridad, el uso o manipulación indebida de los datos. Por otra parte, se recomienda expresamente que no deje el equipo desatendido mientras tenga información importante en la pantalla. Si necesita alejarse del de su computadora aunque sólo sea por un momento, salga de todos los programas y cierre las ventanas que incluyan información importante.

6) PROTECCIÓN DE LA INFORMACIÓN

El área de Sistemas deberá velar por la protección de los datos institucionales generados en los sistemas informáticos administrativos o de gestión. En ese sentido, se deberán implementar políticas apropiadas de backup, cortafuegos (firewall) y antivirus según el tenor de la información y el impacto de los riesgos para todos los servidores administrativos. No está previsto el resguardo de datos de los usuarios en equipos de uso académico.

Por otra parte, es responsabilidad de los usuarios de equipos administrativos el resguardo de la información y datos generados en sus equipos y computadoras personales que se les ha asignado, quienes podrán asesorarse en el área de Sistemas si tuvieran dudas o inconvenientes al realizar sus propios resguardos de información y mantenimiento de antivirus u otros recursos de protección de datos.

La Universidad controla pero no garantiza la ausencia de virus ni de otros elementos que puedan producir alteraciones en los sistemas informáticos, en los contenidos electrónicos o en los archivos almacenados en los equipos de usuarios.

7) PROPIEDAD INTELECTUAL

Los usuarios deben respetar los derechos de propiedad intelectual de los materiales a los que se pueda acceder a través de recursos informáticos, en especial, del Campus Virtual y mecanismos de comunicación virtual tales como blogs o sitios webs gestionados por el área

de Sistemas, ya sean, dichos materiales, propiedad de la Universidad, de los miembros de la comunidad universitaria o de terceros.

Los contenidos, imágenes o documentos colocados en un aula del Campus Virtual, sitios Web o blogs no pueden ser objeto de reproducción, distribución, comunicación pública o transformación no autorizada. Se exceptúa la posibilidad de que el usuario copie en su computadora o imprima una copia de los materiales a los cuales puede acceder para su propio uso personal, es decir, para usarlos como materiales de estudio, investigación o gestión.

No está permitido colocar en las aulas virtuales, sitios web o blogs material académico que surja de la reproducción total o parcial de publicaciones no propias de las cuales no se cuente con licencia o autorización expresa de sus autores. Todo material académico no propio que se coloque en las aulas o medios virtuales de comunicación deberá reconocer los créditos de la obra de la manera especificada por el autor o el licenciador.

8) USO DE LOS RECURSOS

8.1 Uso del Software

No se permite a los usuarios la instalación de software, ni la modificación del existente en las computadoras institucionales sin consentimiento expreso del Área de Sistemas y Tecnologías.

Los estudiantes sólo podrán realizar copia de software disponible en el área de Sistemas o en Biblioteca, siempre que el mismo sea versión académica o de libre distribución.

La actualización del software de los laboratorios es cuatrimestral y se realiza de manera programada. Por tal motivo, los docentes deben solicitar los recursos que utilizarán en el transcurso de sus asignaturas con antelación al inicio de las clases. Es muy importante, en este sentido, que los Directores de Departamento o Coordinadores académicos soliciten al Área de Sistemas y Tecnologías, con anterioridad al inicio de clases, los recursos que utilizarán los docentes, según sus planificaciones académicas.

Se menciona expresamente como acción que incumple con esta normativa la violación de los términos de las licencias de software adquiridos por la Universidad o de los convenios y contratos firmados con las empresas proveedoras de software y de servicios informáticos.

8.2 Programación y uso de los recursos informáticos

Para disponer de recursos informáticos de uso académico el docente debe contar con la autorización del Coordinador de su Carrera.

Todos los recursos informáticos de uso académico deben, además, ser reservados. Para ello, los docentes y demás usuarios deben haber solicitado su reserva indicando tipo de recurso, día, hora y asignatura o evento, en tiempo y forma, según lo indicado por el área de Bedelía.

El área de Sistemas y Tecnologías no tiene obligación de ser idóneo en el uso de los programas que se

utilizan en las instalaciones de la Institución ni puede garantizar soporte técnico de manera permanente en todas en las aulas o laboratorios. Por tal motivo, quien solicita recursos debe tener pericia en su utilización o contar con algún auxiliar que la tenga.

Es responsabilidad de los usuarios de recursos informáticos probar el equipamiento asignado con anterioridad al inicio de las actividades ejecutando las aplicaciones y archivos que se utilizarán para evitar problemas de compatibilidad, de versión o configuración que son frecuentes cuando se utilizan equipos distintos a aquellos en los que se escribieron o crearon archivos de datos, de texto, con imágenes o sonidos.

Asimismo, es obligación del docente prever alternativas académicas para el caso de que, por fuerza mayor, no pueda contar con los recursos tecnológicos.

Cuando los requerimientos de recursos superen en cantidad a los disponibles, se dará intervención a los Señores coordinadores de carreras a fin de que determinen las prioridades académicas de los requerimientos.

Cuando sea un alumno quien requiera algún recurso informático adicional a los puestos a su disposición para uso libre y a los ya asignados, deberá solicitarlo previo contar con la autorización expresa del coordinador de la carrera. Le caben en este caso, las mismas responsabilidades mencionadas para el docente relacionadas con la reserva del recurso, la pericia en el uso de los mismos y las pruebas previas.

8.3 Uso de los laboratorios y computadoras académicas

La capacidad de los laboratorios está determinada por la cantidad de computadoras que alberga, incluidas aquellas que estén transitoriamente en reparación. No está permitida la conformación de comisiones o grupos de trabajo que asistan concurrentemente al laboratorio que excedan en más del 10% de su capacidad, sin autorización expresa del área de Sistemas y Tecnologías.

Por cuestiones de protección y de mantenimiento de los equipos, los usuarios no deben dejar sin autorización del área de Sistemas y Tecnologías archivos de trabajo en los equipos académicos sino, almacenarlos en dispositivos de almacenamiento portátiles (disquete, CD, DVD, flash disks, pendrives, etc.). El área de Sistemas y Tecnologías no garantiza la seguridad y protección de la información almacenada en dichos equipos en ningún caso. Incluso, se recomienda mantener copia actualizada en forma permanente de los archivos personales en los dispositivos de almacenamiento portátiles mientras se está trabajando con ellos, en especial, en oportunidad de las evaluaciones.

8.4 Uso de la red de datos

La red de datos está configurada como intranets integrada por subredes administrativas y académicas. No está permitido conectar equipos administrativos a las subredes académicas ni viceversa sin la intervención del área de Sistemas y Tecnologías.

No está permitido conectar dispositivos repetidores ni concentradores, de cables o inalámbricos ni el uso de bocas de conexión de red sin la autorización expresa y supervisión

del área de Sistemas en ninguna de las subredes.

La capacidad de transmisión de datos de las redes informáticas es limitada; los usuarios tienen la obligación de usar la red de datos con economía ya que, siendo un recurso compartido, cualquier uso abusivo puede conllevar la saturación y merma de disponibilidad del servicio para los restantes usuarios.

Por tal motivo, no están permitidas las transferencias de datos excesivas o muy voluminosas de carácter no justificado o que puedan comprometer la normal actividad de la Universidad y se sugiere que los archivos remotos sean consultados y editados, preferentemente, en copias locales a fin de evitar tráfico innecesario en la red, toda vez que esto sea posible.

8.5 Uso de Internet

La Universidad se reserva el derecho de analizar las trazas de navegación por Internet de los usuarios bajo indicios de sospecha o denuncia de mal uso de los recursos, con el fin de evitar el incumplimiento de esta normativa, así como también, el de establecer filtros limitativos para garantizar la seguridad y buen uso de los servicios.

No está permitida para uso personal la sintonización de emisoras de radio o televisión a través de Internet, el uso de programas o sitios Web para hacer Chat (IRC, Internet Relay Chat) así como tampoco la descarga o distribución de archivos de audio y video que no sean de uso académico o institucional.

Cuando cuestiones institucionales o propias de las actividades académicas ameriten el uso de alguno de estos recursos, el área de Sistemas evaluará la viabilidad de brindar el servicio.

La Institución no garantiza la disponibilidad y continuidad del funcionamiento de ningún servicio basado en el uso de Internet y no se responsabiliza por los cortes de conexión originados en los enlaces remotos. En consecuencia, los usuarios deben prever alternativas para cuando no sea factible el acceso a los servicios de Internet.

Estas reservas y limitaciones se aplican tanto para Internet alámbrica (por las intranets) como inalámbrica (servicio institucional de WiFi)

8.6 Uso del campus virtual

Las aulas virtuales se habilitan por pedido de los docentes, quienes deben haber incluido su utilización en la planificación académica y haber realizado la solicitud de apertura de aula en tiempo y forma. Se describe a continuación el perfil deseable del docente responsable de un aula virtual:

-Tener pericia en el uso de computadoras y estar familiarizado con el uso del campus virtual ya sea porque lo utilizó antes o porque realizó previamente de manera satisfactoria un curso de autoaprendizaje.

-Comunicarse con habitualidad mediante el correo electrónico y acceder a una conexión a Internet sin dificultad (en su hogar, en su oficina, en la propia institución, etc.).

-Estar dispuesto a comunicarse mediante una o más herramientas virtuales (cartelera, email, foro, blog, etc.) con sus alumnos y a establecer con ellos un compromiso de respuestas (por ejemplo, qué herramientas va a utilizar, con qué frecuencia va a responder consultas virtuales, etc.).

-Tener digitalizado, preferentemente mediante archivos del tipo .pdf., el material de trabajo, apuntes, documentos, etc. que desea proporcionar a sus alumnos, los cuales no deben incumplir con lo estipulado en el presente reglamento.

8.7 Uso de medios virtuales abiertos

Se entiende por medio virtual abierto todo ámbito que, utilizando medios informáticos o de telecomunicaciones produce el efecto de representación de una realidad (por ejemplo, un sitio Web, un blog, un wiki, un grupo de trabajo informático, una comunidad o red social basada en Internet, etc.) para el cual el área de Sistemas y Tecnologías no determina qué usuarios están habilitados para acceder y cuáles son sus permisos.

La Universidad no se responsabiliza por los medios virtuales abiertos ni por los contenidos allí vertidos que pudieran utilizar miembros de la comunidad educativa.

Sin embargo, los responsables del uso del medio virtual abierto, en tanto son miembros de la comunidad educativa, deben avenirse a esta y a toda normativa vigente en la Universidad.

8.8 Uso del correo electrónico

El correo electrónico es considerado un medio de comunicación institucional. Por esta razón, la información que se envía mediante este medio se considera oficialmente comunicada.

Toda comunicación institucional realizada a través de correo electrónico debe realizarse por una casilla de correo institucional (de los servidores de correo caece.edu.ar o ucaecemp.edu.ar), asignada a una persona o área.

Se puede hacer uso tanto del Webmail como de servicios POP y SMTP mediante software de correo.

Se recomienda especialmente no abrir ningún archivo adjunto si no se conoce al remitente y no se esperaba el mensaje. En su lugar, eliminarlo de inmediato. Se sugiere también no responder mensajes de correo que soliciten información personal o claves de acceso, le informen sobre problemas en sus cuentas o le soliciten actualizar sus datos personales. Estos mails, conocidos como “phishing”, son, generalmente, fraudulentos.

8.8.1 Titularidad de una cuenta

Las casillas de correo electrónicas pueden ser asignadas a una persona (personal de gestión o administrativo, docente, alumno o terceros autorizados) o a un área. En este último caso, se considera titular de la misma al responsable del área quien debe decidir quien o quienes la utilizarán.

En caso de que el titular de una cuenta asignada a un área determine que la misma debe ser utilizada por otras personas, transferirá el uso y no la responsabilidad sobre la cuenta. En consecuencia, debe establecer cuál es el destino que se le dará al uso de la cuenta, si los usuarios deben identificarse personalmente o como integrante del área al establecer una comunicación, etc.

8.8.2 Limitaciones al uso del correo electrónico

El manejo que se haga del correo electrónico debe estar en un todo de acuerdo con el presente reglamento y se deja indicado expresamente que no está permitida la utilización o generación de correo comúnmente llamado basura, la realización de spam, el envío de cadenas de mail, o cualquier otro tipo de publicidad sin consentimiento expreso de las autoridades de la Universidad.

Es decir, está prohibido hacer uso abusivo del correo electrónico, lo cual implica que:

- El correo electrónico no debe ser usado para la difusión de contenido inadecuado, es decir, aquel que constituya complicidad con hechos delictivos. Los mensajes que se envíen y la información adjunta no pueden ser cuestionables u ofensivos, tal como establece el presente reglamento en deberes de los usuarios.
- La difusión de mensajes no debe realizarse a través de canales no autorizados (no está permitido, por ejemplo, utilizar una casilla ajena para reenviar correo propio).
- No está permitida la difusión masiva no autorizada de mensajes (situación que se daría en el caso de uso de casillas propias o ajenas para enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado) ni ataques con objeto de imposibilitar o dificultar el servicio.

La Universidad no es responsable del contenido de las comunicaciones abusivas emitidas por un usuario a través del correo electrónico ni del contenido de correos que este pueda recibir.

Los usuarios son completamente responsables de todas las actividades realizadas a través de sus cuentas de correo electrónico, debiendo tomar conciencia de los términos, prohibiciones y perjuicios eventuales que puedan surgir del uso abusivo, desde el momento en que dichas cuentas son de titularidad de la Universidad.

En este sentido, cuando existan requerimientos legales o haya sospechas fundadas de quebrantamiento del respeto institucional o se sospeche de actividades que puedan acarrear responsabilidades legales a la Universidad, las autoridades están facultadas para acceder y controlar toda la información que circule por las cuentas de correo institucional.

Se recomienda que el envío masivo de mensajes (aun cuando no configuren spam) sea realizado por múltiples mensajes, no incluyendo a más de 12 destinatarios por envío.

Es responsabilidad del usuario mantener el espacio asignado a su cuenta de correo libre borrando o bajando los mensajes a su computadora personal.

Se recomienda borrar periódicamente el contenido de la bandeja de elementos eliminados y

no mantener en la bandeja de entrada o de salida excesiva cantidad de mensajes.

8.8.3 Baja de las cuentas de correo electrónico

En el caso de que se sospeche uso abusivo de una cuenta de correo, podrá darse de baja preventivamente la cuenta. En caso de verificarse la falta, además, de poder darse de baja definitivamente la cuenta, se aplicará la normativa vigente según el tenor de la misma, pudiendo derivar en una sanción disciplinaria. Las casillas de correo electrónica también podrán ser dadas de baja sin que medie aviso ni tiempo si cesa o cambia la vinculación de su titular con la Universidad.

En el caso de las casillas de correo electrónica asignadas a un área, en lugar de ser dadas de baja por desvinculación de la persona a la cual estaba asignada, la Universidad se reserva el derecho de reasignarla a otro usuario responsable. En este último caso, se le asignará a la casilla de correo una nueva clave de acceso.

8.8.4 Limitaciones del servicio

Aunque en un porcentaje muy elevado de casos los mensajes de correo electrónico llegan a su destino rápidamente, en ningún caso el servicio de correo garantiza la entrega de un mensaje. Numerosas circunstancias pueden impedir la recepción de un mensaje: desde caídas imprevistas en las líneas de comunicaciones propias de los proveedores de Internet involucrados en una comunicación, el límite de espacio disponible en la casilla de correo del usuario receptor, rechazo del mensaje por virus o por el tipo de archivo adjunto, etc.

Con el fin de optimizar el servicio de correo, se podrán establecer limitaciones en la prestación relacionadas con el tamaño máximo de un mensaje enviado, tamaño máximo de casilla, es decir, espacio en disco disponible para almacenar mensajes, número máximo de destinatarios por mensaje, etc.

En todos los casos, se informará al usuario de tales limitaciones al momento de abrirse una nueva casilla de correo o cuando se modifiquen.

Todos los mensajes de correo electrónico serán analizados por el antivirus del Servidor de correo (actualizado a diario). Si el sistema encontrara algún mensaje o archivo adjunto infectado, el mismo podrá ser borrado.

Esto no exime al usuario de tomar las medidas necesarias para proteger su computadora personal: instalar un antivirus y mantenerlo actualizado, desconfiar y borrar mensajes no solicitados, no abrir mensajes sospechosos, etc.

El Servidor de correo también analiza los mensajes tratando de detectar correo basura (SPAM) y etiquetará aquellos mensajes que se consideren SPAM. Además, se podrán establecer filtros limitativos de tipo de archivo adjunto con el fin de intentar garantizar la seguridad y buen uso del servicio de correo electrónico.

8.9 Sitio Web Institucional

Todo sitio Web oficial de la Universidad se considera un medio de comunicación Institucional a disposición de la comunidad universitaria y de todos los interesados.

Los Sitios Web institucionales que proporcionen un nivel de seguridad basado en información de acceso a áreas restringidas (destinadas, por ejemplo, a la autogestión) están especialmente abarcados por el ítem 4, Seguridad en el acceso, e ítem 5, Confidencialidad de la información.

Algunos servicios de Autogestión, además, pueden ser establecidos como la vía habitual o normal de realización de trámites o gestiones para alumnos, docentes y personal administrativo.

8.10 Uso del teléfono

La Universidad se reserva el derecho y así lo informa expresamente de monitorear mediante el sistema de comunicación telefónica las llamadas entrantes y salientes pudiendo quedar registrados para las llamadas entrantes, los números telefónicos externos que se comuniquen a cada interno, tipo de llamada, día y hora de inicio de la comunicación y cantidad de rings producidos antes de recepcionada la comunicación y, para las llamadas salientes, la identificación del usuario, el número telefónico que el usuario marque, día y hora de inicio de la comunicación, duración de la llamada y tipo de llamada, con fines de seguridad institucional y de facilitación la gestión de los recursos de comunicación.

9 Incumplimiento de la normativa

El incumplimiento de estas normas de uso y conductas podrán dar lugar a que se apliquen sanciones disciplinarias según el Reglamento de Disciplina y Código de Ética de la Universidad (R.R. Nº 113/09). Si llegara a extremos punibles a nivel jurídico, la Universidad tomará las medidas que considere oportunas tanto a nivel administrativo y civil como penal que, según la legislación vigente, correspondiera.

Los usuarios que intencionalmente hagan mal uso de los recursos y deterioren o sustraigan algún equipo serán pasibles, además, de sanciones que pueden incluir tanto la prohibición del uso como afrontar el costo de la reparación o reposición de la pieza dañada o sustraída, el cual podrá ser cargado a la cuenta corriente del usuario o descontado de haberes, sin perjuicio de otras medidas disciplinarias, académicas o legales.

En los casos en que la gravedad del problema amerite una sanción disciplinaria sin que medie advertencia, el área de Sistemas y Tecnologías elevará el caso para su tratamiento a las autoridades de la Universidad. En estos casos, el área de Sistemas también podrá aplicar al usuario, de manera preventiva, la baja como miembro de la comunidad virtual, la suspensión de uno más servicios prestados y/o el bloqueo temporal del acceso.



UNIVERSIDAD
CAECE
SEDE MAR DEL PLATA



Bolsa de Comercio
de Mar del Plata