UNIVERSIDAD METROPOLITANA DE CIENCIAS DE LA EDUCACIÓN

CONTRALORIA INTERNA RECEPCION		
CONTROL JURIDICO		
REGISTRO DE PERSONAL		
REGISTRO CONTABLE		
REGISTRO DEBIENES		
REGISTRO REG. DPTO.:R.		
REFRENDACION		
REF.POR $_____ IMPUTAC._____ ANOT.POR $_____ IMPUTAC._____		
DEDUC._____		

APRUEBA LAS POLITÍCAS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD METROPOLITANA DE CIENCIAS DE LA EDUCACIÓN.

RESOLUCIÓN EXENTA N° 2022-00-0164

SANTIAGO, 28 de febrero de 2022

VISTOS:

Lo dispuesto en la Ley N° 18.433; en el D.F.L. N° 1 de 1986 del Ministerio de Educación; en el Decreto Supremo del Ministerio de Educación N° 87/2021; y en la Resolución N° 7/2019 de la Contraloría General de la República.

CONSIDERANDO:

1° Que, la Jefa del Departamento de Informática de la Universidad Metropolitana de Ciencias de la Educación, mediante Memorándum N°14/2022, de 20 de enero de 2022, dirigido a Secretaría General, adjunta las políticas de informática de la Universidad Metropolitana de Ciencias de la Educación, presentadas en el marco del proyecto de Calidad UMC 1857, con referencia al HITO “OE2, Fortalecer el área de informática para la gestión institucional a través de políticas, condiciones de operación e implementación de sistemas”.

2° Que, por Acuerdo N°1042 adoptado por la Junta Directiva de la Universidad en sesión especial vía remota, de fecha 19 de enero de 2022, se aprobaron las Políticas de Tecnologías de la Información de la UMCE., y las se adjuntan por Memorándum N°35 de fecha 20 de enero de 2022, de Secretaría General con la solicitud de aprobarlas mediante el respectivo Acto Administrativo.

RESUELVO:

1º Apruébense las Políticas de Tecnologías de la Información la Universidad Metropolitana de Ciencias de La Educación, sancionadas mediante Acuerdo N°1042, de la Junta Directiva de fecha 19 de enero de 2022, conforme el documento adjunto, denominado Políticas Tecnologías de la Información de la Universidad Metropolitana de Ciencias de La Educación, cuyo tenor es el siguiente:

PABLO ANDRES CORVALAN REYES

Firmado digitalmente por PABLO ANDRES CORVALAN REYES
Fecha: 2022-03-01 16:53:21

PABLO CORVALAN REYES
SECRETARIO GENERAL

UNIVERSIDAD METROPOLITANA
DE CIENCIAS DE LA EDUCACIÓN
SECRETARÍA GENERAL

Acuerdo 1042

SECRETARÍA GENERAL

JUNTA DIRECTIVA

Sesión ordinaria vía remota del 19 de enero del 2022

VISTOS : Las atribuciones de la Junta Directiva, establecidas en el Estatuto de la UMCE, DFL N° 1 de 1986, Artículo 13°, letra b.

CONSIDERANDO :

- La propuesta de la Jefa del Departamento de Informática.

ACUERDO N° 1042 : La Junta Directiva, reunida en sesión ordinaria vía remota del 19 de enero del 2022, aprueba, por unanimidad, las **Políticas Tecnológicas de la Información**, cuyos documentos descriptivos forman parte integrante del presente Acuerdo.

PABLO ANDRES CORVALAN REYES
Firmado digitalmente por PABLO ANDRES CORVALAN REYES
Fecha: 2022.01.20 22:52:31 -03'00'

PABLO CORVALÁN REYES
SECRETARIO GENERAL

POLÍTICAS TECNOLOGÍAS DE LA INFORMACIÓN

UNIVERSIDAD METROPOLITANA DE CIENCIAS DE LA

EDUCACIÓN

Agosto 2021

POLÍTICA DE CLASIFICACIÓN DE RIESGOS DE SISTEMAS Y DATOS ELECTRÓNICOS

1. Declaración de política

La Universidad Metropolitana de Ciencias de la Educación, en adelante UMCE, se compromete a salvaguardar la privacidad de sus estudiantes, exalumnos, académicos, funcionarios y visitantes, así como a proteger la confidencialidad, integridad y disponibilidad de información y sistemas que son importantes para la misión de la Universidad.

2. Objeto de esta política

Esta política proporciona un marco para salvaguardar los activos de información de la UMCE, es decir, sus sistemas de tecnología de la información y los datos que posee. UMCE ha clasificado sus activos de información en categorías basadas en riesgos, con el fin de determinar quién tiene permiso para acceder y utilizar esos activos y qué medidas de seguridad deben tomarse para salvaguardarlos contra el acceso no autorizado o la violación de la confidencialidad, integridad o disponibilidad (triada de la información). Esta política debe leerse junto con la Política de seguridad de datos y sistemas, que establece las medidas de seguridad específicas que se aplican a cada clasificación de datos y sistemas.
Esta política establece las siguientes clasificaciones de riesgo para los datos de la UMCE: riesgo bajo, riesgo moderado y riesgo alto; y las siguientes clasificaciones de criticidad para los sistemas: Criticidad baja, Criticidad moderada y Criticidad alta. Las clasificaciones ayudan a identificar el nivel de protección requerido para cualquier tipo específico de datos o sistema. Si bien todos los datos y sistemas deben protegerse, se requieren medidas más estrictas a medida que aumenta el nivel de riesgo o criticidad.

3. Alcance

Los datos y sistemas a los que se hace referencia en esta política deben protegerse adecuadamente independientemente de la ubicación de los datos específicos y los sistemas en los que se pueden encontrar. Esta clasificación de riesgo, por lo tanto, es aplicable a una amplia variedad de recursos de TI que están conectados o se utilizan para cualquier propósito comercial dela UMCE, incluidos los dispositivos de propiedad personal. Un "sistema" se define como cualquier recurso de TI al que se pueden aplicar salvaguardias de seguridad.
Los ejemplos de sistemas incluyen:

1. Computadoras de escritorio, portátiles o servidores que ejecutan sistemas operativos de propósito general como Windows, Mac OS, Unix / Linux y aplicaciones móviles.
2. Aplicaciones de servidores de red, como una aplicación de servidor SFTP.
3. Aplicaciones y aplicaciones web, como sistemas de información para estudiantes, sistemas de recursos humanos, sistemas de gestión del aprendizaje, sitios web, CMS y wikis, entre otros.
4. Bases de datos, almacén de datos (dw), API y otros sistemas de intercambio de datos (como Box, Dropbox, Drive, OneDrive).
5. Dispositivos móviles, como tabletas, teléfonos inteligentes y dispositivos de IoT donde se pueden almacenar datos.
6. Sistemas de autenticación y autorización como SSO (single sign-on), Active Directory y LDAP, entre otros.

Todos los sistemas anteriores pueden realizar su propia autenticación y autorización, registro y auditoría, y tener sus propias configuraciones que deben ser administradas, y cada uno de ellos se considera un objeto de cumplimiento a salvaguardar.

Un sistema puede clasificarse con una criticidad más alta que la requerida por la clasificación siguiente. Si es así, el sistema debe cumplir con las medidas de seguridad para el nivel de criticidad más alto.

4. A quién se aplica esta política

Los responsables de clasificar los datos y el riesgo del sistema pueden ser propietarios de sistemas individuales, administradores de sistemas, gerentes de proyectos, administradores de bases de datos o administradores de datos. Toda la comunidad de la UMCE (cuerpo docente, funcionarios, estudiantes, contratistas, consultores, ex alumnos, proveedores e invitados) que acceden a los datos y sistemas de la Universidad debe considerar cómo están protegiendo los datos y sistemas de la Universidad. Por lo tanto, todos deben ser conscientes de la sensibilidad de los datos a los que acceden y las consecuencias adversas si esos datos no están debidamente protegidos.

5. Procedimientos para la implementación

5.1. Clasificación de riesgo de datos

A continuación, se describen tres niveles de clasificación de riesgo de datos que se basan en el impacto de un acceso no autorizado, divulgación o alteración de los datos en cuestión a miembros individuales de la comunidad y / o a la UMCE como institución.
La clasificación de riesgo de los datos tiene en cuenta:

- Atributos inherentes de los datos,
- Fuente de los datos,
- Regulación o política que rige los datos, y
- Relación de los datos con los datos divulgados previamente.

La clasificación de datos específicos está sujeta a cambios a medida que cambian los atributos de esos datos (por ejemplo, sus elementos, contenido, usos, importancia, método de transmisión o contexto regulatorio).
Las clasificaciones de datos se enumeran a continuación con ejemplos proporcionados en lasiguiente sección. Deben aplicarse las siguientes reglas al clasificar datos:
Cuando un elemento de datos cae en más de una categoría, debe clasificarse en la categoría de riesgo más alta aplicable. Por ejemplo, si un elemento de datos cumple la definición de datos de riesgo moderado y de riesgo alto, debe clasificarse como de riesgo alto.
Cuando un conjunto de datos incluye más de un elemento de datos, el conjunto de datos debe clasificarse en función de la categoría de riesgo más alta aplicable. Por ejemplo, si una base de datos contiene datos de riesgo bajo y de riesgo moderado, la base de datos debe clasificarse como de riesgo moderado.
Los datos pueden clasificarse con un riesgo mayor que el requerido por las clasificaciones siguientes; si ese es el caso, el elemento de datos debe cumplir con las medidas de seguridad para el nivel de clasificación superior.

Riesgo Bajo	**Riesgo moderado**	**Riesgo Alto**

Los datos se clasifican como riesgo bajo si se aplica alguna de las siguientes condiciones: 1. Los datos generalmente están disponibles para el público, o 2. El uso, acceso o alteración no autorizados de los datos no tendría un impacto adverso en la UMCE o en un miembro individual de la comunidad.	Los datos se clasifican como riesgo moderado si se aplica alguna de las siguientes condiciones: 1. Los datos se rigen por leyes o reglamentos que restringen el uso o la divulgación de dichos datos, o 2. Los datos estánsujetos a restricciones contractuales que restringen el uso o la divulgación de dichos datos, o 3. El uso, acceso o alteración no autorizados de los datos podría tener un impacto adverso en la UMCE o en un miembro individual de la comunidad.	Los datos se clasifican como riesgo alto si se aplica alguna de las siguientes condiciones: 1. Los datos se rigen por leyes o regulaciones que requieren que la UMCE informe a la autoridad competente y / o notifique a las personas si se violan los datos, o 2. El uso, acceso o alteración no autorizados de los datos podría tener un impacto adverso significativo en la UMCE o en un miembro individual de la comunidad.

Un **"impacto adverso"** significa;

i con respecto a un individuo, que la seguridad o privacidad de los datos se ha visto comprometida con un probable aumento en el riesgo.

ii con respecto a la UMCE, que los aspectos financieros, legales, operativos, y / o el riesgo de reputación aumentan hasta e incluyendo graves repercusiones.

Ejemplos de riesgo de datos

Los siguientes ejemplos están destinados a ayudar a determinar qué clasificación de riesgo es apropiada para un tipo particular de datos y no están destinados a ser una lista exclusiva de datos que se incluyen en cada clasificación.
Nota sobre los datos de investigación:

1. Datos protegidos relacionados con la investigación: datos de investigación que se rigen por la reglamentación o los requisitos del patrocinador: según el tema y los datos a los que se accede, se generan y / o se comparten, puede haber requisitos más estrictos, del patrocinador o del gobierno.

2. A excepción de los datos regulados, como la información médica protegida, los números de la cédula de identidad, número de pasaporte, los números de cuentas financieras y otros datos protegidos relacionados con la investigación y los sistemas que sirven como repositorios para estos tipos de datos, los datos de investigación se incluyen predominantemente en la clasificación de riesgo bajo.

Riesgo Bajo	Riesgo moderado	Riesgo Alto
Los datos se clasifican como riesgo bajo si se aplica alguna de las siguientes condiciones: 1. Información autorizada para estar disponible en o a través de los sitios web de la UMCE sin autenticación. 2. Manuales de políticas y procedimientos designados por el propietario como públicos. 3. Ofertas de trabajo. 4. Información de contacto de la universidad no	Los datos se clasifican como riesgo moderado si se aplica alguna de las siguientes condiciones: 1. Números de identificación de la universidad y del funcionario. 2. Datos de investigación institucional no publicados (a discreción del propietario) 3. Propiedad intelectual de la UMCE con licencia de un	Los datos se clasifican como riesgo alto si se aplica alguna de las siguientes condiciones: 1. Números de identificación nacional (cédula) y número de documento 2. Números de licenciade conducir. 3. Números de pasaporte y visa. 4. Contraseñas del sistema operativo, contraseñas de aplicaciones y claves API.
designada por la persona como "privada" en el directorio de la UMCE. 5. Mapas del campus disponible al público. 6. Datos de investigación (a discreción del propietario de los datos).	tercero o que está restringida por contrato. 4. Registros de estudiantes y solicitudes de admisión. 5. Datos de recursos humanos (por ejemplo, solicitudes de empleo de docentes / personal, archivos de personal, información sobre beneficios, salario, fecha de nacimiento, información de contacto personal, etc.) 6. Contratos no públicos, conforme a la ley. 7. Memos y correos electrónicos internos oficiales de la UMCE, informes y políticas no públicas, presupuestos, planes, Información de ingeniería, diseño y operaciónrelacionada con la infraestructura de la UMCE. 8. Datos financieros de la Universidad (es decir, datos financieros en el sistema de registro, donde la modificación de esos datos afectaría los procesos de la Universidad.	5. Credenciales de autenticación central. 6. Información de salud protegida. 7. Datos de investigación no publicados que son identificables: datos de investigación institucional no publicados, incluidos datos de investigación no publicados que están sujetos a requisitos de datos protegidos por patrocinadores o gobierno, incluidos datos que se originan por las personas o datos que son confidenciales o sensibles. 8. Números de identificación de la póliza de seguro. 9. Números de tarjetasde crédito / débito y otros datos de titulares de tarjetas. 10. Números de cuenta bancaria. 11. Exportar información controlada.

5.2. Clasificación de riesgo de datos

La criticidad del sistema se determina de acuerdo con las siguientes clasificaciones. Las siguientes reglas se tienen en cuenta al clasificar sistemas:
Cuando un sistema entra en más de una categoría, debe clasificarse en la categoría de criticidad aplicable más alta. Por ejemplo, si una aplicación cumple la definición de criticidad moderada y de alta criticidad, debe clasificarse como de alta criticidad.
Cuando un sistema incluye más de un recurso, el sistema debe clasificarse según la categoría de criticidad aplicable más alta. Por ejemplo, si un sistema incluye aplicaciones de Criticidad baja y Criticidad moderada, debe clasificarse como un sistema de Criticidad moderada.

Criticidad baja	**Criticidad moderada**	**Criticidad alta**
Un sistema se clasifica de criticidad baja cuando cumple con el siguiente criterio: Almacena, transmite o proporciona acceso a datos de bajo riesgo únicamente.	Un sistema se clasifica de criticidad moderada cuando cumple cualquiera de los siguientes criterios: 1. Almacena, transmite o proporciona acceso a datos de riesgo moderado 2. La pérdida de acceso podría tener un impacto significativo en una gran cantidad de usuarios o múltiples unidades de negocios y el riesgo institucional general por el tiempo de inactividad.	Un sistema se clasifica de criticidad alta cuando cumple cualquiera de los siguientes criterios: 1. Almacena, transmiteo proporciona acceso a datos de riesgo alto. 2. La pérdida de acceso podría tener un impacto significativo en la UMCE en su conjunto y el riesgo general de la institución por el tiempo de inactividad.

Ejemplos de criticidad del sistema

Los siguientes ejemplos están destinados a ayudar a determinar qué clasificación es apropiada para un tipo particular de sistema.

Criticidad baja	**Criticidad moderada**	**Criticidad alta**
Un sistema se clasifica de criticidad baja si se aplica alguna de las siguientes condiciones. 1. Aplicaciones que manejan datos de riesgo bajo. 2. Mapas online. 3. Catálogo en línea dela universidad que muestra descripciones de cursos académicos. 4. Directorio público que contiene números de teléfono y direcciones de correo electrónico de los funcionarios de la UMCE.	Un sistema se clasifica de criticidad moderada si se aplica alguna de las siguientes condiciones. 1. Aplicaciones que manejan datos de riesgo moderado. 2. Aplicación de recursos humanos que almacena información salarial. 3. Aplicación universitaria que distribuye información sobre incidentes en caso de emergencia en el campus. 4. Sistema que contiene información relacionada con solicitudes de empleo.	Un sistema se clasifica de criticidad alta si se aplica alguna de las siguientes condiciones. 1. Aplicaciones que manejan datos de riesgo alto. 2. Aplicación de recursos humanos que almacena los datos de los funcionarios 3. Aplicación que procesa pagos contarjeta de crédito.

Dependiendo de los niveles de clasificación determinados para datos y sistemas, los procedimientos para proteger los sistemas se describen en Política de seguridad de datos y sistemas

5.3. Clasificación de riesgo de datos

Apéndice a: definición de acrónimos

AD: se refiere a Active Directory, desarrollado originalmente para redes de dominio de Windows que administran permisos y acceso a un directorio de servicios de red.
API: se refiere a la interfaz de programación de aplicaciones, un sistema de intercambio de datos que recibe solicitudes y envía respuestas.
CMS: se refiere a un sistema de gestión de contenido, como WordPress.
RRHH: se refiere a los sistemas de Recursos Humanos de la UMCE.
IoT: se refiere al Internet de las cosas, un sistema en expansión de dispositivos informáticos físicos, mecánicos y digitales interrelacionados, con identificadores únicos (es decir, una dirección IP para la conectividad a Internet) y capaz de comunicarse y transferir datos a través de una red entre estos objetos y otros dispositivos de Internet. Dispositivos y sistemas habilitados sin necesidad de interacción de persona a persona o de persona a computadora.
IP: significa Protocolo de Internet, una dirección única asignada a todos los dispositivos informáticos en una red para la identificación de la interfaz y la ubicación con el fin de que se comuniquen con otros dispositivos informáticos en esa red.
LDAP: significa Protocolo ligero de acceso a directorios, un procedimiento de software para permitir la ubicación de organizaciones, personas y otros recursos, como archivos y dispositivos, ya sea una Internet pública o una intranet organizacional, y puede comunicarse con Active Directory.
Linux: sistema operativo de código abierto y de uso general que se utiliza en una gran cantidad de plataformas y dispositivos de hardware.
Mac OS: se refiere al sistema operativo de propósito general Macintosh desarrollado, comercializado y vendido por Apple Inc. para computadoras personales.
SFTP: significa aplicación de servidor Secure File Transfer Protocol y es una versión segura del File Transfer Protocol (FTP), que facilita el acceso y la transferencia de datos a través de un flujo de datos Secure Shell (SSH).
SSO: significa solución de inicio de sesión único, una propiedad del control de acceso para garantizar que solo los usuarios autorizados tengan acceso a datos confidenciales.
Unix: sistema operativo patentado de uso general con licencia con usos de investigación, académicos e incluso comerciales y un poderoso modelo de diseño de software modular.
Windows: se refiere a un grupo de varios sistemas operativos gráficos de propósito general para computadoras personales, desarrollados, comercializados y vendidos por Microsoft.

Control de versiones

Autor	**Fecha**	**Versión**	**Motivo**
Trends	20/01/2021	V00	Creación
UMCE – Trends	14/05/2021	V01	Modificación
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE CORREO ELECTRÓNICO

1. Objeto y resumen

Esta Política establece la aplicación de las políticas de la Universidad Metropolitana de Ciencias de la Educación, en adelante UMCE, al correo electrónico (e-mail).
La Universidad reconoce que los principios de libertad académica, libertad de expresión, privacidad y confidencialidad tienen implicaciones importantes para el correo electrónico y los servicios de

correo electrónico. Esta Política aborda estos principios dentro del contexto y sujeto a las limitaciones impuestas por las obligaciones legales y políticas de la Universidad.

2. El propósito de esta Política es asegurar que:

La comunidad universitaria utilizará el correo electrónico de manera ética y considerada de conformidad con las leyes y políticas aplicables, incluidas las políticas establecidas por la Universidad y sus unidades operativas, y con respeto por la confianza pública a través de la cual se han proporcionado estas instalaciones;
Los usuarios de correo electrónico están informados sobre cómo los conceptos de privacidad y seguridad se aplican al correo electrónico, así como la aplicabilidad de las políticas y leyes pertinentes; y
Minimizar las interrupciones en el correo electrónico de la Universidad y otros servicios y actividades.

3. Alcance

Esta política se aplica a:

Todos los servicios de correo electrónico proporcionados, propiedad o financiados en parte o en su totalidad por la Universidad;
Todos los usuarios y titulares de cuentas o sistemas de correo electrónico de la Universidad, independientemente del uso previsto; y
Todos los Registros Oficiales de correo electrónico de la Universidad y / o Registros Públicos en posesión o generados por los funcionarios de la Universidad y otros usuarios de los servicios de correo electrónico proporcionados por la Universidad, independientemente de si los registros se generaron en computadoras de la Universidad o computadoras externas de la Universidad.
Esta Política se aplica igualmente a los datos de transmisión y recepción, incluidos los encabezados de los correos electrónicos, los resúmenes y las direcciones asociadas con los registros de correo electrónico, y cualquier archivo o texto adjunto.

Esta política no se aplica a:

Servicios de Internet distintos del correo electrónico
Mensaje de voz
Conferencias de audio y video
Mensajes de fax
Las copias impresas del correo electrónico, pero es posible que se apliquen otras normas o leyes y políticas a dichos documentos.

4. POLÍTICA

i. Disposiciones de uso específico

Prestación de servicios: las unidades organizativas de la Universidad pueden proporcionar servicios de correo electrónico en apoyo den la docencia, investigación y servicio público de la Universidad.
Propiedad de la Universidad: Los servicios de correo electrónico se extienden para el uso exclusivo del funcionamiento universitario, funcionarios, estudiantes y otros usuarios autorizados de la Universidad para realizar tareas relacionadas y consistentes con la misión de la Universidad. Los sistemas y servicios de correo electrónico de la Universidad son instalaciones, recursos y propiedad de la Universidad, tal como se utilizan esos términos en las políticas de la Universidad y la ley aplicable. Cualquier dirección de correo electrónico o cuenta asignada por la Universidad a personas, subunidades o funciones de la Universidad son propiedad de la Universidad.

ii. Restricciones de servicio autorizado

Los usuarios de correo electrónico deben cumplir con las leyes, las políticas de la Universidad y los estándares normales de cortesía y conducta profesional y personal. El acceso a los servicios de correo electrónico de la Universidad puede ser restringido total o parcialmente por la Universidad sinprevio aviso y sin el consentimiento del usuario del correo electrónico: (a) cuando así lo requiera y sea consistente con la ley o política aplicable; (b) cuando existe una sospecha razonable de que se han producido o pueden producirse infracciones de la política o la ley; o (c) cuando sea necesario para satisfacer necesidades operativas críticas independientes del tiempo. Dichas restricciones de acceso están sujetas a la aprobación de la autoridad supervisora o administrativa de la Universidad (por ejemplo, jefes de departamento, jefatura de informática, etc.). Las unidades operativas autónomas de la Universidad deben establecer o identificar estos niveles de autoridad.
Las unidades operativas de la universidad pueden definir "Condiciones de uso apropiado" adicionales para instalaciones de red y computación locales para complementar esta Política con detalles, pautas o restricciones adicionales. Dichas condiciones deben ser coherentes con esta Política y estar subordinadas a ella, y están destinadas a abordar principalmente situaciones de suministro de recursos limitado.
Cuando finaliza la afiliación de un individuo a la Universidad, la Universidad puede intentar redirigir el correo electrónico durante un período de tiempo razonable según lo determine para propósitos consistentes con esta Política y la misión de la Universidad. La Universidad puede optar porcancelar la cuenta de correo electrónico de la persona o continuar con la cuenta, sujeto a la aprobación de la autoridad operativa de sistemas y supervisión de la Universidad correspondiente.

iii. Acceso y divulgación autorizados

La Universidad puede permitir la inspección, monitoreo o divulgación de correo electrónico cuando:

1. Existe una sospecha razonable de que se han producido o pueden ocurrir violaciones de la ley o de la política de la Universidad;
2. Hay necesidades operativas críticas dependientes del tiempo de los negocios de la Universidad si la Universidad determina que la información buscada no está disponible más fácilmente por otros medios o,
3. Cuando existan requerimientos legales que obliguen a la universidad a entregar dicha información.
4. En otros casos debidamente fundamentados y por razones del buen servicio universitario.

En tales casos, la Universidad, como cortesía, normalmente tratará de informar a los usuarios de correo electrónico antes de cualquier inspección, monitoreo o divulgación de registros de correo electrónico, excepto cuando dicha notificación sea perjudicial para una investigación de una posible violación de la ley o política universitaria. Los usuarios deben cumplir con las solicitudes de la Universidad para acceder a los registros de correo electrónico y obtener copias de ellos cuando la ley o esta política aplicable requiera o permita el acceso o la divulgación, independientemente de si dichos registros residen en una computadora alojada o propiedad de la Universidad. El incumplimiento de tales solicitudes puede dar lugar a acciones disciplinarias u otras accioneslegales de conformidad con la ley o política aplicable, incluidas, entre otras, las políticas de personal de la Universidad o los códigos de conducta apropiados.

Indemnización de la Universidad: Los usuarios acuerdan en virtud del acceso a los sistemas informáticos y de correo electrónico de la Universidad, indemnizar, defender y mantener indemne a la Universidad por cualquier demanda, reclamación, pérdida, gasto o daño, incluidos, entre otros, litigios, costos y honorarios de abogados, que surjan o estén relacionados con el acceso del usuario o el uso del correo electrónico y los sistemas, servicios e instalaciones informáticos de la Universidad.

iv. Mal uso

1. El uso del correo electrónico para actividades ilegales está estrictamente prohibido. El uso ilegal puede incluir, entre otros, obscenidad; pornografía, pornografía infantil; amenazas; acoso; robo; intentar el acceso no autorizado a los datos o intentar violar cualquier medida de seguridad en

cualquier sistema de comunicaciones electrónicas; intentar interceptar cualquier transmisión de comunicación electrónica sin la debida autoridad; y violación de las leyes de derechos de autor, marcas comerciales o difamación.

2. El incumplimiento de la ley que conlleve la comisión de ilícitos sancionados penalmente . El robo o destrucción no autorizada, alteración, falsificación o eliminación de registros de correo electrónico puede dar lugar a cargos por delitos tipificados algunos de ellos en la ley N°19.223, que tipifica figuras penales relativas a la Informática.

3. Además de las actividades ilegales, las siguientes prácticas de correo electrónico están expresamente prohibidas: ingreso, examen, uso, transferencia y alteración de las cuentas y archivos de otros, a menos que estén debidamente autorizados de conformidad con esta política; alterar el software del sistema de correo electrónico o las configuraciones de hardware; o interferir con el trabajo de otros o con la Universidad u otras instalaciones informáticas.

4. Si otro usuario ha solicitado a un usuario por correo electrónico o por escrito que se abstenga de enviar mensajes de correo electrónico, el destinatario tiene prohibido enviar a ese usuario más mensajes de correo electrónico hasta el momento en que haya sido notificado por el administrador del sistema que dicha correspondencia está permitida. El incumplimiento de dicha solicitud se considerará una violación de esta Política.

5. Los servicios de correo electrónico de la Universidad no se pueden utilizar para actividades comerciales que no estén aprobadas por el personal competente y designado por las autoridades de la Universidad de acuerdo con la política aplicable; ganancia financiera personal (excepto según lo permitido por las políticas académicas aplicables); uso personal inconsistente con la Sección III de esta política; usos que violen otras políticas o pautas de la Universidad; o usos incompatibles con la ley aplicable. Las políticas de la Universidad aplicables incluyen, entre otras, políticas y pautas con respecto al personal, la propiedad intelectual o la discriminación y el acoso.

6. Los usuarios de correo electrónico no darán la impresión de que están representando, dando opiniones o haciendo declaraciones en nombre de la Universidad o de cualquier unidad de la Universidad a menos que estén expresamente autorizados para hacerlo. Cuando corresponda, se incluirá una exención de responsabilidad explícita.

7. Los servicios de correo electrónico de la universidad no se utilizarán para fines que razonablemente se pueda esperar que causen, directa o indirectamente, tensión en las instalaciones informáticas o interferencia con el uso de correo electrónico o sistemas de correo electrónico por parte de otros. Dichos usos incluyen, entre otros, el uso de servicios de correo electrónico para:

   a. Enviar o reenviar correos en cadena.

   b. "Correo no deseado"; es decir, explotar listservs o sistemas similares para la distribución generalizada de correo no solicitado.

   c. mail-bomb ó "correo-bomba"; es decir, reenviar el mismo correo electrónico repetidamente a uno o más destinatarios.

El mal uso del correo institucional acarreara la responsabilidad civil, penal o administrativa según corresponda.

v. Uso personal

Los servicios de correo electrónico de la universidad se pueden utilizar para fines personales incidentales siempre que dicho uso no:

1. Interfiera directa o indirectamente con el funcionamiento de las instalaciones informáticas o los servicios de correo electrónico de la Universidad.

2. Interfiera con el empleo del usuario del correo electrónico u otras obligaciones con la Universidad.

3. Viole esta Política, o cualquier otra política o ley aplicable, incluido, entre otros, el uso para beneficio personal, conflicto de intereses, acoso, difamación, violación de derechos de autor o actividades ilegales.

Sin embargo, los mensajes de correo electrónico que surjan de dicho uso personal estarán sujetos a acceso de conformidad con esta política o la ley aplicable. En consecuencia, dicho uso no conlleva privacidad.

vi. Confidencialidad

1. No se puede garantizar la confidencialidad del correo electrónico, y cualquier confidencialidad puede verse comprometida por el acceso consistente con la ley o política aplicable, incluida esta Política, por redistribución no intencional o debido a tecnologías actuales inadecuadas para proteger contra el acceso no autorizado. Los usuarios, por lo tanto, deben tener extrema precaución al usar el correo electrónico para comunicar asuntos confidenciales o sensibles, y no deben asumir que su correo electrónico es privado o confidencial.

2. Los usuarios no pueden acceder, usar o divulgar información personal o confidencial sin la debida autorización, y deben tomar las precauciones necesarias para proteger la confidencialidadde la información personal o confidencial, independientemente de si la información se mantiene en papel o se encuentra en el correo electrónico u otros registros electrónicos.

3. Los administradores de sistemas no cuentan con los privilegios para acceder a las cuentas de correo de la universidad.

vii. Seguridad y preservación

1. Los usuarios y operadores de correo electrónico deben seguir prácticas correctas y sólidas para garantizar la seguridad de los registros, datos, programas de aplicaciones y programas desistemas de correo electrónico bajo su jurisdicción.
2. Los usuarios y operadores deben protegerse contra el deterioro de los medios de almacenamiento y la inaccesibilidad a los registros de correo electrónico debido a la obsolescencia del hardware o software. Para eliminar estas situaciones, los usuarios debenprever la accesibilidad futura;
    a. Migrar todos los registros oficiales de correo electrónico a la próxima generación de hardware o software; o
    b. Migrar solo los registros de correo electrónico oficiales actuales a un nuevo hardware o software, o convertir los registros de correo electrónico oficiales no migrados a otros medios (p. ej., disco óptico, cloud) para almacenamiento a corto plazo o en "formatolegible a simple vista" (p. o microfilm) para almacenamiento y conservación a largo plazo.
3. Los usuarios son responsables de salvaguardar su nombre de usuario (ID) y contraseña (password), y de usarlos solo según su autorización. Cada usuario es responsable de todas las transacciones de correo electrónico realizadas bajo la autorización de su ID y de toda la actividad de correo electrónico de la red que se origine con su identificación. Está prohibido el uso de identificaciones de usuario de correo electrónico con fines comerciales. El acceso a las identificaciones de los usuarios **no se puede prestar ni vender. sea en forma gratuita o realizar actividades lucrativas u onerosas**.
4. Cada unidad operativa debe establecer:

a. Estándares para la identificación de registros oficiales de correo electrónico y la organización de archivos.

b. Medidas para proteger el correo electrónico oficial confidencial almacenado electrónicamente.

c. Procedimientos para la copia de seguridad de archivos.

viii. Infracciones

Las violaciones sospechadas o conocidas de la política o la ley deben informarse de manera confidencial al nivel de supervisión apropiado para la unidad operativa en la que ocurre la violación. Las infracciones serán procesadas por las autoridades universitarias adecuadas y / o las agencias policiales. Las violaciones pueden resultar en la revocación de los privilegios del servicio de correo electrónico; deshonestidad académica o procedimientos del código de conducta; en el ejercicio de una acción disciplinaria (investigación sumaria), respecto del personal universitario, en cuanto a los y las estudiantes, hasta el sumario disciplinario respectivo y en todos los casos si existe mérito, el ejercicio de acciones legales.

ix. APÉNDICE A: PRECAUCIONES GENERALES DE USO

Los usuarios deben tener en cuenta lo siguiente:

a. Tanto la naturaleza del correo electrónico como el carácter público de los negocios de la Universidad hacen que el correo electrónico sea menos privado de lo que los usuarios pueden anticipar. Por ejemplo, el correo electrónico destinado a una persona a veces puede distribuirse ampliamente debido a la facilidad con que los destinatarios pueden reenviarlo a otras personas. Una respuesta a un mensaje de correo electrónico publicado en un tablón de anuncios electrónico o "servidor de listas" destinado únicamente al autor del mensaje puede distribuirse a todos los suscriptores del servidor de listas. Además, incluso después de que un usuario elimina un registro de correo electrónico de una computadora o cuenta de correo electrónico, puede persistir total o parcialmente en los registros del sistema, en los directorios de la persona que recibió el mensaje o en los servidores de respaldo del sistema, donde pueden conservarse durante largos períodos de tiempo. Todos estos elementos pueden estar sujetos a divulgación según esta Política. La Universidad no puede proteger habitualmente a los usuarios contra tales eventualidades.

b. El correo electrónico, independientemente de que se haya creado, recibido o almacenado en el equipo de la Universidad, puede constituir un "Registro oficial"; puede ser un "Registro Público" sujeto a divulgación o acceso en virtud de otras leyes o como resultado de un litigio.

c. La Universidad no cumple automáticamente con todas las solicitudes de divulgación, pero intenta evaluar dichas solicitudes contra las disposiciones precisas de la Ley con respecto a la divulgación y la privacidad.

d. La Universidad, en general, no puede ni desea ser el árbitro del contenido del correo electrónico. La Universidad tampoco puede, en general, proteger a los usuarios de recibir correos electrónicos que puedan encontrar ofensivos. Sin embargo, se insta encarecidamente a los miembros de la comunidad universitaria a que utilicen las mismas cortesías y consideraciones personales y profesionales en el correo electrónico que utilizarían en otras formas de comunicación, y en particular las aplicables a las comunicaciones escritas, ya que el correo electrónico crea un registro tangible de esa comunicación.

e. No hay garantía, a menos que se utilicen sistemas de correo "autenticados", de que el correo electrónico recibido haya sido enviado por el presunto remitente, ya que es relativamente fácil, aunque una violación de esta Política, que los remitentes oculten su identidad. Además, el correo electrónico reenviado también puede modificarse. La tecnología de autenticación no se utiliza de forma amplia y sistemática en la Universidad a la fecha de esta Política. Al igual que con los

documentos impresos, en caso de duda, los destinatarios de los mensajes de correo electrónico deben consultar con el presunto remitente para validar la autoría o autenticidad.

f. El cifrado de correo electrónico es otra tecnología emergente que no se usa ampliamente a la fecha de esta Política. Esta tecnología permite la codificación del correo electrónico para que, a todos los efectos prácticos, no pueda ser leído por nadie que no posea la clave correcta.

g. El uso inadecuado del correo electrónico puede exponer a la Universidad y a los usuarios individuales a reclamos por daños por infracción de derechos de autor, difamación, violación de la privacidad u otros derechos personales o de propiedad.

h. La ley y las políticas de la Universidad con respecto a los derechos de autor y la propiedad intelectual se aplican al correo electrónico. No viole los derechos de autor de otros. A menos que se establezca legalmente que el material es de dominio público o que el propietario de los derechos de autor lo haga explícitamente, no puede copiar la información de correo electrónico. Consulte con la autoridad correspondiente antes de asumir que tiene derechos de autor sobre dicho material.

i. Aunque el remitente y el destinatario de un correo electrónico hayan eliminado su correo electrónico, es posible que existan copias de seguridad durante períodos de tiempo y en ubicaciones desconocidas para el remitente o el destinatario. Se puede acceder a estas copias o divulgarlas de conformidad con la política o ley aplicable.

PROHIBICIONES:

Acceder, leer, usar, transferir o manipular cuentas o archivos que no esté autorizado a usar.
Modificar las configuraciones de hardware o software del sistema sin autorización.
Difamar a otros a través del correo electrónico.
Participar en actividades ilegales, tales como hacer amenazas, acoso, robo, violar las medidas de seguridad o violar otras leyes o políticas aplicables.
Participar en actividades comerciales no aprobadas por la autoridad correspondiente.
Participar en actividades para beneficio económico personal, excepto según lo permitan las políticas académicas aplicables.
Violar las políticas y pautas de la Universidad.
Enviar o reenviar cartas en cadena, maliciosas, cartas bomba o spam.

Control de versiones

Autor	Fecha	Versión	Motivo
Trends	20/01/2021	V00	Creación
UMCE – Trends	07/05/2021	V01	Modificación
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE SEGURIDAD DE DATOS Y SISTEMAS

i. Política

Las medidas de manejo de datos y seguridad del sistema incluidas en esta política están diseñadas para proporcionar resistencia frente al panorama de amenazas actual y rápidamente cambiante e incluyen ataques complejos y dirigidos que a menudo se centran en el robo de datos académicos, de investigación y administrativos. Las medidas de seguridad se han creado teniendo en cuenta las mejores prácticas de la industria, los requisitos de cumplimiento externo y la política existente de la UMCE. Debido a que ningún sistema informático es completamente inmune a la explotación, la aplicación de controles de seguridad por capas protege los sistemas de la Universidad, los datos y la información sensible en constante expansión de la UMCE. La Universidad ha implementado esta Política para ayudarlo a proteger y asegurar los datos y los sistemas que están a su cuidado.

Para describir la importancia de los sistemas de tecnología de la información, se describen medidas que representan cuán severo podría ser el impacto para la Universidad si un sistema dado estuviera comprometido o no estuviera disponible para realizar su función. Los sistemas con una clasificación más alta deben cumplir con un estándar de seguridad del sistema más estricto para lograr el cumplimiento. Para aplicar los controles de seguridad adecuados, es responsabilidad de todas las personas que utilizan los recursos informáticos y de datos de la Universidad:

1. **Conocer la clasificación del sistema en uso:** Los sistemas informáticos se clasifican en tres categorías: Criticidad baja, Criticidad Moderada y Criticidad Alta, dependiendo de la criticidad de los datos almacenados en él, transmitidos por él, o los datos a los que proporciona acceso. Véase la Política de clasificación de riesgos de sistemas y datos electrónicos.

2. **Conocer el tipo de datos que se manejan**: Los datos se clasifican en una de tres categorías: Riesgo bajo, Riesgo moderado y Riesgo alto, que se describen en la Política de clasificación de riesgos del sistema y datos electrónicos, y se basan en el riesgo para la Universidad de sudivulgación no autorizada. Además, los datos de investigación pueden tener obligaciones contractuales y legales.

3. **Siga las medidas de seguridad apropiadas contenidas en esta Política de seguridad de datos y sistemas:** Estas medidas describen la estrategia de seguridad multicapa de la UMCE para la defensa contra el acceso no autorizado a los sistemas de la Universidad y el manejo apropiado de datos.

4. **Comprender las formas alternativas de cumplimiento de esta Política:** en algunos casos, un sistema puede ser incapaz de implementar un control requerido por esta Política. En tales casos,la excepción debe ser documentada y aprobada por la autoridad correspondiente. Para los sistemasde alta criticidad administrados por el Departamento de Informática, esto implica una evaluación de riesgos de seguridad y la posterior aprobación de las medidas.

Esta política cubre las siguientes medidas:
Seguridad para el manejo de datos
Seguridad del sistema

ii. Objeto de esta política

Los datos y recursos del sistema a los que se hace referencia en esta Política deben protegerse adecuadamente independientemente de la ubicación de esos recursos. Esta Política se aplica a cualquier persona que acceda, use o controle los recursos informáticos y de datos de la Universidad, incluidos, entre otros, académicos, administradores, funcionarios, investigadores, estudiantes, quienes trabajan en nombre de la Universidad, invitados, contratistas, consultores, visitantes y / o personas autorizadas por instituciones y organizaciones afiliadas.

iii. Alcance

Las medidas descritas en esta Política son aplicables a una amplia gama de recursos de TI que están conectados y se utilizan para cualquier propósito comercial de la UMCE. Un sistema puedeser cualquier recurso de TI al que se puedan aplicar las salvaguardas descritas en esta Política. Los ejemplos de sistemas incluyen:

1. Computadoras de escritorio, portátiles o servidores que ejecutan sistemas operativos de uso general como Windows, macOS, Unix / Linux y aplicaciones móviles, ya sean de propiedad personal o de la UMCE, cuando se utilizan para actividades de la Universidad.
2. Aplicaciones de servidor de red, como una aplicación de servidor SFTP.
3. Aplicaciones y aplicaciones web, como sistemas de información para estudiantes, sistemas de recursos humanos, sistemas de gestión del aprendizaje, sitios web, CMS y wikis, entre otros.
4. Bases de datos, almacén de datos, API y otros sistemas de intercambio de datos.
5. Dispositivos móviles, como tabletas, teléfonos inteligentes y dispositivos de IoT donde se pueden almacenar datos.
6. Sistemas de autenticación y autorización como SSO (single sign-on), Active Directory y LDAP.

Todos los sistemas anteriores pueden realizar su propia autenticación y autorización, registro y auditoría, y tienen sus propias configuraciones que deben ser administradas, y cada uno de ellos se considera un objeto de cumplimiento que debe protegerse.

iv. Medidas de seguridad en el manejo de datos

Requisitos para el manejo de datos de riesgo bajo (datos públicos)
Requisitos para manejar datos de riesgo moderado
Requisitos para manejar datos de riesgo alto
Requisitos adicionales para el manejo de datos de investigación

Descripción de las medidas de seguridad para el manejo de datos

Todo el acceso a los datos se le otorga como parte de su función en la UMCE y esos datos deben protegerse adecuadamente. Estas medidas de Seguridad para el Manejo de Datos definen los requisitos mínimos de seguridad que se deben aplicar a los tipos de datos definidos en la Política de Clasificación de Riesgos de Sistemas y Datos Electrónicos.

1. Requisitos para el manejo de datos de riesgo bajo (datos públicos)

1.1. **Control de acceso**: el acceso a los datos clasificados como de riesgo bajo generalmente está disponible para el público. El uso, acceso o alteración de datos públicos no estará restringido siempre que su divulgación al público no tenga un impacto adverso en la UMCE o en un miembro individual de la comunidad. El público tiene permiso implícito parautilizar los datos que se ponen a su disposición.

1.2. **Compartir:** los datos de bajo riesgo pueden compartirse libremente y pueden divulgarse públicamente sin obtener el permiso de un administrador de datos.

1.3. **Retención:** los datos de bajo riesgo pueden almacenarse durante el tiempo que sea necesario; no existen políticas que rijan la retención de datos públicos.

2. Requisitos para manejar datos de riesgo moderado

2.1. **Control de acceso:** el acceso a los datos de riesgo moderado debe proporcionarse con el mínimo de privilegios. Ninguna persona o sistema debe tener acceso a los datos a menos que lo requiera un proceso. En los casos en que se requiera acceso, el Departamento de Informática debe otorgar el permiso para usar los datos.

2.2. **Compartir**: los datos de riesgo moderado se pueden compartir entre los funcionarios de la Universidad de acuerdo con un proceso bien definido aprobado por el Departamento de Informática. Solo se puede divulgar públicamente de acuerdo con procesos bien definidos y con el permiso del administrador de datos.

2.3. **Retención**: Los datos de riesgo moderado solo deben almacenarse durante el tiempo que sea necesario para lograr la ejecución del proceso.

2.4. **Notificación de incidentes:** si hay un incidente de seguridad potencial que pueda poner los datos de riesgo moderado en riesgo de acceso no autorizado, se debe notificar al Departamento de Informática de forma inmediata.

3. Requisitos para el manejo de datos de alto riesgo

3.1. **Recopilación:** los datos de alto riesgo deben recopilarse solo cuando se cumplan todas las condiciones siguientes:

3.1.1. Los datos no están disponibles de otra fuente autorizada; y
3.1.2. Los datos son requeridos por un proceso; y
3.1.3. Tiene permiso para recopilar los datos del administrador de datos correspondiente; o
3.1.4. Si los datos son solicitados por el Departamento Jurídico en respuesta a un litigio o en circunstancia o como resultado de un procedimiento administrativo.

3.2. **Control de acceso**: las personas deben tener acceso a los datos de alto riesgo con el mínimo de privilegios. Ninguna persona o sistema puede acceder a los datos a menos que lo requiera un proceso documentado. En los casos en que se requiera acceso, el Departamento de Informática debe otorgar el permiso para usar los datos.

3.3. **Auditoría de acceso**: se debe habilitar la auditoría de acceso para archivos que contienen datos de alto riesgo.

3.4. **Etiquetado**: Los medios portátiles que contienen datos de alto riesgo deben estar claramente marcados.

3.5. **Compartir:** el acceso a datos de alto riesgo solo puede ser otorgado por el Departamento de Informática o área responsable de dichos datos. Ninguna persona puede compartir datos de alto riesgo con otra persona a la que un administrador de datos o área responsable no le haya otorgado acceso.

3.6. **Acceso inactivo**: los dispositivos que se pueden usar para acceder a datos de alto riesgo deben bloquearse automáticamente después de un período de inactividad, mediante el uso de contraseñas de salvapantallas, cierre de sesión automático o controles similares.

3.7. **Cifrado de tránsito:** los datos de alto riesgo deben cifrarse durante la transmisión con un método que cumpla con los siguientes requisitos:

3.7.1. Las longitudes de las claves criptográficas cumplen con las mejores prácticas en cuanto a longitud, dadas las capacidades actuales de procesamiento informático.

3.7.2. Se deben verificar tanto el origen como el destino de la transmisión.

3.8. **Cifrado de almacenamiento**: los datos de alto riesgo deben cifrarse mediante algoritmos criptográficos públicos sólidos y longitudes de clave razonables dadas las capacidades actuales de procesamiento informático. Las claves deben almacenarse deforma segura y el acceso a ellas debe proporcionarse con el mínimo de privilegios (consulte la norma ISO 11568 para obtener recomendaciones sobre cómo proteger las claves). Si se usa hash unidireccional en lugar del cifrado reversible, se deben usar salted hash.

3.8.1. Cifre los archivos que contienen datos de alto riesgo utilizando claves o contraseñas diferentes a las utilizadas para el inicio de sesión del sistema.

3.8.2. Cifre los datos almacenados en bases de datos a nivel de columna.

3.8.3. Además del cifrado de archivos y / o bases de datos, implemente el cifrado de disco completo en todas las estaciones de trabajo y / o dispositivos portátiles que contienen datos de alto riesgo.

3.9. **Retención:** Los datos de alto riesgo solo deben almacenarse durante el tiempo que sea necesario para lograr la ejecución del proceso de negocios.

3.10. **Destrucción:** cuando los datos de alto riesgo ya no sean necesarios, deben destruirse de acuerdo con las políticas aplicables, utilizando métodos que sean resistentes a los intentos de recuperación de datos, como las utilidades de destrucción de datos criptográficos, la destrucción de dispositivos físicos en el sitio o la destrucción de datos certificada.

3.11. **Notificación de incidentes**: si hay un incidente de seguridad potencial que pueda poner los datos de alto riesgo en riesgo de acceso no autorizado, se debe notificar al Departamento de Informática al Departamento de Informática de forma inmediata.

4. Requisitos para el manejo de datos de investigación

Por razones de seguridad, privacidad y normativas, quienes crean, administran o almacenan datos de investigación deben estar especialmente en sintonía con su clasificación y las medidas de seguridad adecuadas. Los datos de investigación de riesgo moderado o alto deben almacenarse en dispositivos y sistemas controlados por el Departamento de Informática, y no en dispositivos personales o servicios adquiridos personalmente. Los acuerdos de intercambio de datos deben ser examinados por las unidades universitarias correspondientes. Los investigadores deben hacer todo lo posible para garantizar que los datos estén seguros y disponibles solo para aquellos cuyo acceso esté autorizado.

v. Medidas de seguridad del sistema

Las medidas básicas de seguridad del sistema se aplican a todos los sistemas de la UMCE, independientemente del nivel de criticidad del sistema o la clasificación de los datos en el sistema.
Las medidas intermedias de seguridad del sistema definen las medidas de seguridad que deben aplicarse a los sistemas de criticidad moderada.
Las medidas avanzadas de seguridad del sistema definen las medidas de seguridad que deben aplicarse a los sistemas de alta criticidad.

Requisitos de conformidad

Cuando un sistema cae en más de una categoría de criticidad o incluye aplicaciones o recursos de datos que caen en más de una categoría de riesgo, el sistema siempre debe clasificarse en la categoría de criticidad aplicable más alta. La clasificación de la criticidad del sistema y los ejemplos se explican con más detalle en la Política de clasificación de riesgos del sistema y datos electrónicos.

Los sistemas de baja criticidad pueden ser implementados por recursos de TI locales y ubicados en sus respectivas unidades siempre que estén adecuadamente asegurados y protegidos.

Los sistemas de criticidad moderada, antes de la implementación en producción y el establecimiento de conectividad, deben someterse a una revisión de seguridad realizada por el Departamento de Informática. Dependiendo de los hallazgos, el sistema puede requerir una Evaluación de Riesgos de Seguridad completa. En casos particulares, un sistema de criticidad moderada puede necesitar cumplir con los estándares para un sistema de alta criticidad.

Los sistemas de alta criticidad, antes de la implementación en producción y el establecimiento de conectividad, deben someterse a una evaluación de riesgos de seguridad para su aprobación posterior. Los resultados de la Evaluación de riesgos de seguridad se informarán al Departamento de Informática quien entregará las recomendaciones correspondientes. Los sistemas de alta criticidad deben estar alojados en centros de datos aprobados por la UMCE o en instalaciones de servicios en la nube.

Responsabilidad para los administradores del sistema

Los administradores de sistemas tienen mayores responsabilidades con respecto a los requisitos de cumplimiento para cualquier sistema que administran. Primero, deben clasificar el sistema y los datos que procesa de acuerdo con las políticas de la UMCE, en particular la Política de clasificación de riesgos de sistemas y datos electrónicos; y, luego, aplicar los controles del sistema adecuados, con base en esa clasificación del sistema, entendiendo que las medidas de Seguridad son aditivas. Para minimizar el riesgo de seguridad de TI, se recomienda que los administradores del sistema integren la auditoría de cumplimiento en su marco de auditoría y gestión de inventario existente.

Descripción de las medidas de seguridad

Las siguientes secciones describen las medidas de seguridad del sistema básicas, intermedias y avanzadas. Las medidas son acumulativas y se crean para cada categoría de datos y sistemas. Las siguientes medidas de seguridad se aplican a cualquier sistema utilizado para realizar actividades comerciales, de investigación o de enseñanza en la UMCE. Esto incluye equipos que no son propiedad de la universidad, como sistemas de propiedad personal.

1. Medidas de seguridad básicas del sistema

Las medidas básicas de seguridad del sistema se aplican a todos los sistemas de la UMCE, independientemente del nivel de su sistema o clasificación de datos. Constituyen una línea de base que todos los sistemas deben cumplir. En la medida de lo posible, los dispositivos móviles, como teléfonos y tabletas, deben protegerse con estas medidas de seguridad básicas del sistema. Tenga en cuenta que, para la mayoría de las estaciones de trabajo individuales, estas son las únicas medidas de seguridad que se aplicarán, a menos que el nivel de riesgo de los datos en el sistema requiera una medida de seguridad de nivel superior. Los requisitos son:

1.1. **Protección por contraseña**: todas las cuentas y recursos deben estar protegidos por contraseñas que cumplan con la política de contraseñas.

1.2. **Actualizaciones de software:** la mayoría de los sistemas pueden y deben configurarse para recibir actualizaciones automáticas. Para aquellos sistemas, como los servidores de producción, que pueden requerir un enfoque por fases para las actualizaciones, el proceso y la frecuencia de las actualizaciones deben ser definidas por el administrador de sistemas responsable.

Los sistemas deben estar configurados para actualizar automáticamente el software del sistema operativo, las aplicaciones del servidor (servidor web, servidor de correo, servidor de base de datos, etc.), software cliente (navegadores web, clientes de correo, suites de oficina, etc.) y software de protección contra malware (anti-malware), virus, anti-spyware, etc.

1.3. **Cortafuegos:** los sistemas deben estar protegidos por un cortafuegos que permita solo las conexiones entrantes necesarias para cumplir con los requisitos de los procesos de negocio de ese sistema. Los sistemas cliente que no tienen necesidades comerciales para proporcionar servicios de red deben rechazar todas las conexiones entrantes. Los sistemas que brindan servicios de red deben limitar el acceso a esos servicios al grupo más pequeño y razonablemente manejable de hosts que necesitan comunicarse con ellos.

1.4. **Protección antivirus y antimalware:** los sistemas que ejecutan sistemas operativos Microsoft o macOS deben tener software antivirus y antimalware instalado y configurado para escanear y actualizar definiciones automáticamente.

2. Medidas de seguridad del sistema intermedio

Las medidas de Seguridad del Sistema Intermedio definen las medidas de Seguridad que deben aplicarse a los sistemas de Criticidad Moderada y Criticidad Alta. Tenga en cuenta que, excepto en circunstancias especiales, estas medidas no se aplican a computadoras de escritorio o portátiles, ni a dispositivos móviles. Los requisitos son:

2.1. Autenticación y autorización

2.1.1. **Eliminar o deshabilitar cuentas sin uso:** las cuentas que ya no sean necesarias deben deshabilitarse de manera oportuna mediante un procedimiento automatizado o documentado.

2.1.2. **Separar cuentas de administrador (privilegiadas) y de usuario estándar:** las cuentas de administrador (privilegiadas) no se deben utilizar para fines no administrativos. Los administradores del sistema deben contar con cuentas que no sean de administrador para las actividades del usuario final y una cuenta de administrador separada (con privilegios) que se utilice solo para fines de administración del sistema.

2.1.3. **Usar contraseñas únicas para cuentas privilegiadas:** las cuentas privilegiadas deben usar contraseñas únicas que no se comparten entre varios sistemas. Las credenciales que se administran de forma centralizada se consideran una sola cuenta, independientemente de la cantidad de sistemas a los que proporcionen acceso.

2.1.4. **Reducir los intentos repetidos de inicio de sesión fallidos**: siempre que sea posible, se debe aplicar una tasa máxima de intentos fallidos de inicio de sesión. Se requiere el bloqueo de la cuenta después de cinco intentos fallidos de inicio de sesión.

2.1.5. **Habilitar el tiempo de espera de la sesión**: las sesiones de los usuarios deben bloquearse o cerrarse después de 15 minutos de inactividad. En los casos en los que esto sea técnicamente inviable, la sesión de tiempo de espera debe ser lo más breve posible.

2.1.6. **Aplicar el privilegio mínimo:** las cuentas no administrativas deben utilizarse siempre que sea posible. Las cuentas de usuario y los procesos del servidor deben tener el menor nivel de privilegio posible que les permita realizar su función.

2.2. Auditoría y rendición de cuentas

2.2.1. **Sincronizar el reloj del sistema**: El reloj del sistema debe estar sincronizado con un servidor de hora autorizado al menos una vez al día.

2.2.2. **Habilitar el registro y la auditoría del sistema:** las funciones necesarias para generar, retener y caducar automáticamente los registros del sistema deben estar habilitadas.

2.2.3. **Seguir un cronograma de retención de registros adecuado**: Los registros del sistema deben conservarse durante no más de 90 días y luego destruirse, a menos que sea necesaria una retención adicional debido a requisitos reglamentarios o contractuales.

2.2.4. **Auditar inicios de sesión exitosos:** genera un mensaje de registro cada vez que un usuario inicia sesión correctamente.

2.2.5. **Auditar intentos fallidos de inicio de sesión**: genera un mensaje de registro cada vez que un usuario intenta iniciar sesión sin éxito.

2.2.6. **Auditar cuando se inicia o detiene un servicio del sistema:** genera un mensaje de registro cuando se inicia o detiene un servicio del sistema.

2.2.7. **Auditar errores graves o inusuales:** Genere un mensaje de registro cuando se produzca un error grave o inusual, como bloqueos.

2.2.8. **Auditar errores de agotamiento de recursos:** genera un mensaje de registro cuando se produce un error de agotamiento de recursos, como un error de falta de memoria o un error de disco.

2.2.9. **Auditar intentos de acceso fallidos:** genera un mensaje de registro cuando se deniega un intento de acceder a un archivo o recurso debido a privilegios insuficientes.

2.2.10. **Cambiar permisos de auditoría:** genera un mensaje de registro cuando se cambian los permisos de un usuario o grupo.

2.2.11. **Incluir datos de correlación apropiados en los eventos de auditoría:** para cada evento de auditoría registrado, asegúrese de incluir información suficiente para investigar el evento, incluida la dirección IP relacionada, la marca de tiempo, el nombre de host, el nombre de usuario, el nombre de la aplicación y / u otros detalles según corresponda.

2.3. Configuración y mantenimiento

2.3.1. **Partición de seguridad:** los sistemas pueden compartir hardware y recursos solo con otros sistemas que tengan requisitos de seguridad similares, independientemente de su clasificación de criticidad. Los sistemas que comparten requisitos de seguridad similares tienen comunidades de usuarios de tamaño y carácter similares, perfiles de firewallsimilares y requisitos técnicos similares. Por ejemplo:

2.3.1.1. Se pueden agregar varios sistemas de la misma criticidad para compartir hardware y recursos, siempre que tengan requisitos de seguridad similares.

2.3.1.2. Los sistemas de Criticidad moderada pueden compartir hardware y recursos con sistemas de Criticidad baja siempre que todos los sistemas cumplan con las medidas de seguridad de los sistemas intermedios y compartan requisitos de seguridad similares.

2.3.2. **Deshabilitar las cuentas y contraseñas predeterminadas del proveedor**: muchos sistemas vienen con cuentas predeterminadas que son de dominio público. Estas cuentas deben estar deshabilitadas.

2.3.3. **Desactivar todos los servicios de red innecesarios:** los procesos y servicios que no son necesarios para completar la función de un sistema deben desactivarse.

2.4. Requerimientos adicionales

2.4.1. **Informar posibles incidentes de seguridad:** Los incidentes potenciales de seguridad deben informarse al Departamento de Informática de forma inmediata.

2.4.2. **Consultar o evaluar riesgos de seguridad:** antes de la implementación del sistema, el Departamento de Informática debe realizar una evaluación de riesgos de seguridad.

2.4.3. **Evaluar vulnerabilidades:** antes de la implementación del sistema, se debe solicitar una evaluación de vulnerabilidades al Departamento de Informática. Esta evaluación de vulnerabilidades puede implicar un escaneo del sistema.

2.4.4. **Acceso físico:** el sistema debe residir en un centro de datos administrado y seguro, un servicio en la nube o una instalación cerrada a la que solo tenga acceso el personal autorizado.

2.4.5. **Documentar:** cree y mantenga documentación que resuma los procesos de negocio, los principales componentes del sistema y las comunicaciones de red asociadas con un sistema.

3. Medidas de seguridad avanzadas del sistema

Las medidas de seguridad del sistema avanzado definen las medidas de seguridad que se deben aplicar a los sistemas de alta criticidad además de las medidas de seguridad del sistema intermedio. Los requisitos adicionales son:

3.1. Auditoría y rendición de cuentas

3.1.1. **Auditar la escalada de privilegios o el cambio de privilegios:** Genere un mensaje de registro cada vez que un usuario cambie su nivel de privilegio.

3.1.2. **Auditar la denegación del firewall**: genera un mensaje de registro cuando el firewall basado en el host niega una conexión de red.

3.1.3. **Auditar todos los eventos importantes de la aplicación**: registre todos los eventos importantes de la aplicación

3.1.4. **Escribir eventos de auditoría en un sistema separado:** los registros del sistema deben escribirse en un sistema remoto de tal manera que ningún usuario delsistema que se esté registrando pueda modificarlos.

3.2. Configuración y mantenimiento

3.2.1. Cortafuegos basados en host y en red: los sistemas deben estar protegidos tanto por un cortafuegos basado en host como por red que permita solo las conexiones entrantes necesarias para satisfacer las necesidades de ese sistema.

3.2.2. Proceso de gestión de la configuración: los cambios de configuración deben estar regulados por una configuración documentada y un proceso de gestión de cambios.

3.2.3. Partición de seguridad: los sistemas pueden compartir hardware y recursos solo con otros sistemas que tengan requisitos de seguridad similares, independientemente de su clasificación de criticidad. Los sistemas que comparten requisitos de seguridad similares tienen comunidades de usuarios de tamaño y carácter similares, perfiles de firewall similares y requisitos técnicos similares. Por ejemplo:

3.2.3.1. Se pueden agregar varios sistemas de la misma criticidad para compartir hardware y recursos, siempre que tengan requisitos de seguridad similares.

3.2.3.2. Los sistemas de alta criticidad pueden compartir hardware y recursos con sistemas de importancia media y baja, siempre que todos los sistemas cumplan con las medidas de seguridad de sistemas avanzados y compartan requisitos de seguridad similares.

3.3. Requerimientos adicionales

3.3.1. Acceso físico: el sistema debe residir en un centro de datos administrado y seguro o en un servicio en la nube al que solo tendrá acceso el personal autorizado.

Control de versiones

Autor	Fecha	Versión	Motivo
Trends	20/01/2021	V00	Creación
UMCE – Trends	12/05/2021	V01	Modificación
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE CONTRASEÑAS

Propósito

El propósito de esta política es establecer un estándar de uso de contraseñas seguras, la protección de esas contraseñas y su frecuencia de cambios.

Alcance

Esta política se aplica a todos los miembros de la comunidad universitaria que utilizan los recursos informáticos y de datos de la UMCE y / o que tienen acceso a datos confidenciales enviados, transmitidos, vistos, recibidos o almacenados en estos recursos.

Requerimientos de las contraseñas

Esta política requiere que las contraseñas tengan un mínimo de ocho (8) caracteres de longitud, contengan al menos una letra minúscula, una letra mayúscula, un número y un símbolo.

Expiración de las contraseñas

Las contraseñas caducan/expiran a los 365 días.
Se mostrará un aviso de vencimiento al iniciar sesión 30 días antes del vencimiento.

Contraseñas del servicio de correo

Las contraseñas del servicio de correo se pueden cambiar desde el acceso personal a Gmail por parte del usuario.
El administrador puede cambiar la contraseña desde la consola de administración de Google Suite previa solicitud mediante un correo electrónico a correo@umce.cl que quedará como respaldo.

Contraseñas de Sistemas de información

Para cambiar la contraseña en cualquier sistema de información de la UMCE debe comunicarse con el administrador del sistema enviando un correo con copia a la unidad responsable de la administración de dicho sistema.

Bloqueo de cuenta

Si una cuenta se ha bloqueado debido a demasiados intentos fallidos de inicio de sesión o porque ha caducado, debe enviar un correo a correo@umce.cl para obtener ayuda.

Recomendaciones

Aunque tenga una contraseña segura, cambiarla con frecuencia agrega otra capa de seguridad. Cuanto más tiempo esté vinculada la misma contraseña a una cuenta de usuario, mayor será la probabilidad de que alguien la conozca o pueda adivinarla.

Si cree que alguien conoce su contraseña, cámbiela inmediatamente. Debe proteger su contraseña con tanto cuidado, tal como lo hace con el PIN de su tarjeta de cajero automático. Nunca escriba su contraseña junto a su computadora o en algún lugar donde otra persona pueda encontrarla fácilmente.

No debe ser una palabra del diccionario, un nombre propio o el nombre o las iniciales de una persona.

Esto generará aleatoriamente una contraseña que puede utilizar. Las contraseñas se basan en palabras del diccionario para que sean más fáciles de recordar, pero se han modificado para que otros no las adivinen. La barra de seguridad de la contraseña le permitirá saber si la contraseña que eligió es muy débil, débil, buena o segura.

Reutilizar contraseñas. Proteja sus cuentas de usuario UMCE, así como todas sus otras cuentas personales, con contraseñas únicas. La reutilización de contraseñas lo pone en riesgo en caso de que se vulnere una cuenta, ya que los estafadores intentarán piratear otras cuentas con las credenciales que han robado.

No use su nombre de usuario, nombre o apellido. Su nombre y nombre de usuario se almacenan en el archivo de contraseñas y muchos programas de piratería utilizan esta información paragenerar posibles combinaciones de contraseñas.

No use el nombre ni el apellido de nadie. Muchos programas para descifrar contraseñas tienen grandes bases de datos de nombres y pueden adivinar fácilmente las contraseñas basándose en los nombres. Los nombres de amigos, familiares, personajes de ficción, etc., se asocian comúnmente con un individuo y no crean contraseñas seguras.

Palabras escritas al revés. Las palabras escritas al revés no constituyen contraseñas seguras. La mayoría de los programas de craqueo intentan la representación hacia adelante y hacia atrás de las palabras en sus bases de datos y, por lo tanto, las contraseñas de este tipo no son seguras.
Sustituir 1 y 0 por 1 y o no es suficiente para crear una contraseña segura. Los programas para descifrar contraseñas tienen conjuntos de reglas diseñados para romper contraseñas que sustituyen números por letras que se parecen.

Palabras simples. No utilice simplemente una palabra seguida o precedida por un número como contraseña. Un algoritmo común para adivinar contraseñas agrega números al principio o al final de una palabra del diccionario. Por lo tanto, las contraseñas de esta forma se descifran fácilmente. Se deben utilizar caracteres no alfabéticos en toda la contraseña.

Uso de diccionarios. No utilice diccionarios o palabras basadas en diccionarios como contraseñas. Los programas de descifrado de contraseñas tienen diccionarios grandes que utilizan para adivinar las contraseñas. También tienen grandes diccionarios de idiomas extranjeros; por lo tanto, el uso de palabras extranjeras como contraseñas no es seguro.

Contraseñas de ejemplo. Nunca use una contraseña que se haya citado como ejemplo de cómo elegir una contraseña segura.

Nunca le entregue a nadie su contraseña. Ni siquiera si dicen ser administradores de sistemas o personal de soporte. Compartir contraseñas es una violación de la política de la UMCE, y el personal de informática nunca pedirá la suya. Si alguien a quien le proporciona su contraseña usara su cuenta de manera inapropiada, podría ser considerado responsable de sus acciones. Si necesita delegar sus credenciales de acceso, comuníquese con el Departamento de Informática al correo correo@umce.cl para obtener ayuda.

No enviar contraseñas por correo. Nunca envíe su contraseña por correo electrónico a usted mismo ni a nadie más.
Existen programas que tienen la capacidad de espiar el tráfico enviado a través de Internet. Si envía un mensaje con su contraseña, existe la posibilidad de que sea interceptado y su cuenta se vea comprometida.

Su contraseña no debe tener todos los números, letras mayúsculas o minúsculas, ni debe tener caracteres repetidos.

Patrones de teclado. Las contraseñas que utilizan patrones en el teclado, es decir qwerty, no son seguras. Aunque estas contraseñas se escriben fácilmente, también se adivinan fácilmente.

Requisitos de complejidad de clave

Estos requisitos son válidos tanto para el servicio de correo como para todos los sistemas de información nuevos y los ya existentes en la Universidad.
Las contraseñas deben cumplir los siguientes requisitos de complejidad:

- ✓ Mínimo de ocho (8) caracteres de longitud.
- ✓ Debe incluir al menos uno de cada uno de los siguientes:
  - o letras (a-z y / o A-Z)
  - o al menos un número (0-9)
  - o al menos un carácter especial: *! @ # 0 ^ & * _ - = [] | ; ~,. /?

Las contraseñas deben ser únicas y no deben usarse para ninguna otra cuenta. Las contraseñas anteriores no se pueden reutilizar.

Control de versiones

Autor	Fecha	Versión	Motivo
Trends	08/01/2021	V00	Creación
Departamento Informática	29/04/2021	V01	Revisión
UMCE – Trends	07/05/2021	V02	Revisión
UMCE – Trends	23/06/2021	V03	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE CUMPLIMIENTO DE LICENCIAS DE SOFTWARE

i. Propósito

El propósito de esta Política es subrayar la importancia del cumplimiento de las disposiciones de licencia de software y definir responsabilidades específicas relacionadas con este cumplimiento.

ii. Alcance

Esta Política se aplica a toda la Universidad.

iii. Definiciones

DI – Departamento de Informática

iv. Contenido

1. Antecedentes

El incumplimiento de las disposiciones sobre licencias de software puede generar un riesgo y una responsabilidad importantes para la Universidad. Las auditorías externas de software en universidades de Chile para identificar el incumplimiento no son infrecuentes, y el costo para las universidades que se encuentran en incumplimiento puede ser considerable.

Es muy importante que la Universidad cuente con procesos robustos para asegurar que cuenta con las licencias necesarias y adecuadas para todo el software que utiliza y que cumple con las condiciones de uso estipuladas en las licencias. El no hacerlo pone a la Universidad en riesgo significativo de ser sujeta a acciones legales y sanciones sustanciales.

2. Política

(a) La responsabilidad de asegurar el cumplimiento de la licencia de software recae en la jefatura del Departamento de Informática.

Las responsabilidades específicas son:

(i) mantener un registro para proporcionar prueba de la compra del software.

(ii) mantener un registro de eliminación de software a través de la venta (por ejemplo, software vendido con una computadora).

(iii) mantener un inventario que detalle dónde se instala el software con licencia. Esto debe permitir rastrear la redistribución de software dentro de la universidad.

(iv) asegurarse de que todo el personal sea consciente de sus propias responsabilidades con respecto a garantizar que solo utilicen software de conformidad con las condicionesde la licencia.

(b) Con el fin de garantizar el cumplimiento de los requisitos de licencia, los jefes de área, departamentos o facultades pueden, de vez en cuando, iniciar una auditoría de cumplimiento del software.

(c) Todo software sin licencia será removido del o los computadores en que se encuentre, se dejará un registro y se informará a la jefatura inmediata de la persona infractora, operador o operadora del Departamento de Informática y al Departamento jurídico (como resguardo).

(d) El único documento que acredita legalidad del software es la factura de compra correspondiente. El Departamento de Informática deberá tener un registro digital de todas las facturas de compra de software, tales como; Microsoft Office, MS SQL Server, VMware, etc.

Control de versiones

Autor	Fecha	Versión	Motivo
Trends	20/01/2021	V00	Creación
UMCE – Trends	07/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE DESARROLLO DE SOFTWARE

i. Propósito

El propósito de esta Política es estandarizar el desarrollo de software para todas las aplicaciones web mediante el uso de prácticas líderes en la industria. Estas aplicaciones y servicios normalmentetratan con todos los sistemas de información con que cuenta la UMCE, y se requiere la debida diligencia en la protección de estos datos. Estandarización del enfoque de desarrollo y las técnicas de codificación para los sistemas garantizarán su mantenibilidad, seguridad, protección contra los ciberataques y la accesibilidad.

ii. Alcance

Esta Política se aplica a todos los funcionarios, estudiantes, docentes, consultores y / o contratistas involucrados en el desarrollo o modificación de aplicaciones que apoyan la gestión de la UMCE.
Si alguna disposición de esta Política es incompatible con las normas generales aplicables en la materia, prevalecerán dichas normas y la Política se entenderá ajustada a dichas normas.

iii. Política

El Departamento de Informática es responsable de desarrollar, mantener y participar en el Ciclo de vida de desarrollo de sistemas o "SDLC" (System Development Life Cycle) para proyectos de desarrollo de aplicaciones de la UMCE. Todo software desarrollado internamente que se ejecuta en sistemas de producción debe desarrollarse de acuerdo con el SDLC. Como mínimo, esta política

aborda las áreas de; análisis preliminar, estudio de factibilidad, identificación y mitigación de riesgos, análisis de sistemas, especificación de diseño, desarrollo, aseguramiento de la calidad, test de aceptación, implementación, postimplementación, mantenimiento y revisión. Esta metodología asegura que el software se documentará y probará adecuadamente antes de que sea utilizado por la UMCE.
Todas las aplicaciones desarrolladas en o para la UMCE deben cumplir los estándares y procedimientos de desarrollo documentados en la Política de desarrollo de software y Guía de estándares de desarrollo de aplicaciones. Estos estándares incluyen: técnicas de codificación, estrategias de prueba, documentación, requisitos y procesos de lanzamiento de software que se alinean con estándares de la industria.
Debe haber una separación entre la producción, entornos de desarrollo y prueba. Esto asegurará que la seguridad se mantiene rigurosamente para los sistemas en producción, mientras que los entornos de desarrollo y prueba pueden maximizar la productividad con menos restricciones de seguridad. Las restricciones establecidas para el personal de desarrollo y prueba no deben permitir el acceso a los sistemas en producción.

iv. Definiciones

Aplicación. Programas informáticos, procedimientos, reglas, documentación asociada y datos pertenecientes a la operación de un sistema informático.
Misión crítica. Un sistema o aplicación cuya falla resulta en caída o falla de las operaciones de la Universidad.
Ciclo de vida de desarrollo del sistema(software) (SDLC). Un proceso estandarizado para planificar, crear, probar e implementar una aplicación.

v. Cumplimiento

Todas las aplicaciones se revisan en puntos de control predeterminados del SDLC por el arquitecto de software o su designado. Se identifican las desviaciones y se determina la acción correctiva antes de que la aplicación sea lanzada a producción. La autorización electrónica que indica que se han cumplido los estándares es necesaria antes de que se pueda lanzar una aplicación nueva o modificada a producción.
Informática hace cumplir esta Política y los Estándares relacionados en todo momento. Cualquiera que tenga motivos para sospechar un acto deliberado y / o violación de esta política se recomienda que la infracción de esta Política sea inmediatamente informada Departamento de Informática.
Se evaluarán las infracciones de las políticas y se tomarán medidas para remediarlas, estas violaciones están sujetas condiciones contractuales.
Cuando las infracciones de la política se consideran graves y / o no pueden remediarse fácilmente, el incidente se derivará a la jefatura de informática y jurídica si corresponde para futuras acciones. Periódicamente, informática hará un resumen de todas las violaciones de políticas, las cuales se encontrarán debidamente registradas en un sistema informático para su seguimiento.

Control de versiones

Autor	Fecha	Versión	Motivo
Trends	25/02/2021	V00	Creación
UMCE – Trends	17/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE DISPOSITIVOS MÓVILES

i. Propósito

Asegurar la compra y el uso adecuados de los dispositivos móviles conectados al plan móvil de la Universidad.

ii. Alcance

Esta política se aplica a todos los dispositivos móviles y / o cuentas de dispositivos móvilesfinanciadas por la Universidad.

iii. Definiciones

Dispositivo móvil Cualquier dispositivo que se conecte a una red celular (por ejemplo, teléfono móvil, tableta, tarjeta SIM o dispositivo de datos móvil).

Dispositivo móvil universitario Un dispositivo móvil comprado por la universidad.

Dispositivo móvil externo Un dispositivo móvil no comprado por la Universidad.

Cuenta de dispositivo móvil La provisión y registro de servicios y uso de un dispositivo móvil específico. El ciclo de vida de la cuenta comienza con la compra del dispositivo y finaliza cuando se cancelan todos los servicios, se devuelve el dispositivo y se cumplen los compromisos de costos finales.

Titular del dispositivo móvil La persona que es el usuario principal del dispositivo móvil.

Patrocinador del dispositivo móvil La persona responsable del presupuesto de los costos de compra y / u operación del dispositivo móvil.

Proveedor aprobado Un proveedor / vendedor de servicios con el que la Universidad tiene un acuerdo de suministro negociado formalmente.

Proveedor aprobado de servicios móviles El proveedor aprobado para servicios de dispositivos móviles (por ejemplo, mensajes de voz SMS / txt y datos).

Plan móvil universitario El servicio del dispositivo móvil y las opciones de uso seleccionadas por la Universidad y proporcionadas por el proveedor de servicios móviles aprobado.

iv. Contenido

1. Elegibilidad

Los funcionarios pueden recibir un dispositivo móvil si sus responsabilidades universitarias requieren:
(a) que utilicen un dispositivo móvil en sus actividades diarias,

(b) deben ser accesibles inmediatamente,

(c) están de turno de llamado fuera del horario normal de funcionamiento,

(d) a menudo no se encuentran en un lugar de trabajo fijo y deben ser fácilmente contactables ó

(e) hacen viajes frecuentes y / o prolongados fuera de su campus de origen.

2. Compra de un dispositivo móvil universitario

a) La autoridad para aprobar el suministro de un dispositivo móvil a un funcionario recae en el director de la Dirección de Administración y Finanzas (DAF).

(b) Los teléfonos móviles universitarios, las tarjetas SIM y los dispositivos de datos móviles deben comprarse a través del área de compras.

(c) Los dispositivos móviles de la universidad deben comprarse a un proveedor aprobado para la adquisición.

(d) El dispositivo móvil que se va a comprar debe ser el modelo más rentable que permita al usuario llevar a cabo de manera eficiente sus tareas relacionadas con el trabajo.

(e) El Departamento de Informática publicará una lista de dispositivos móviles aceptables y la revisarán periódicamente.

3. Uso y seguridad

(a) Los dispositivos móviles de la Universidad deben utilizar el plan móvil de la Universidad. Las excepciones a esto deben ser aprobadas por el Departamento de Informática.

(b) Los dispositivos móviles externos pueden utilizar el plan móvil de la Universidad con la aprobación del Departamento de Informática con la condición de que la Universidad pueda instalar software y configurar el dispositivo móvil externo con fines de seguridad, recuperación de dispositivos y cumplimiento de las obligaciones de licencia.

(c) Los números de teléfono móvil se publicarán en los directorios de la Universidad, a menos que existan razones específicas de seguridad / privacidad por las que no deberían publicarse.

(d) Los titulares de dispositivos móviles siempre deben operar dispositivos móviles de manera segura y legal.

(e) Los titulares de dispositivos móviles deben tomar todas las medidas prácticas para evitar la pérdida o daños de sus dispositivos móviles.

(f) El titular del dispositivo móvil es responsable de la seguridad de los datos de la Universidad almacenados en el dispositivo móvil.

(g) Los dispositivos móviles deben estar bloqueados cuando no estén en uso mediante el uso de un PIN, contraseña, datos biométricos u otra funcionalidad de seguridad similar.

(h) Se monitoreará el uso de todos los dispositivos móviles en el plan móvil de la Universidad.

(i) Todos los dispositivos móviles del plan móvil de la Universidad deben estar configurados para conectarse a la red WiFi de la Universidad.

(j) La Universidad puede instalar software y configurar sus dispositivos móviles con fines de seguridad, recuperación de dispositivos y cumplimiento de las obligaciones de licencia.

(k) Los titulares de dispositivos móviles de la universidad deben informar, tan pronto como sea posible, la pérdida / robo de un dispositivo móvil. Cuando esto es:

i. Dentro del horario laboral normal, informe la pérdida al Departamento de Informática para proceder al bloqueo del dispositivo.

ii. Fuera del horario laboral normal, informe la pérdida / robo directamente al proveedor (la empresa de telecomunicaciones o proveedor de los servicios) de servicios móviles aprobado para bloquear el uso de voz, SMS y / o datos en la cuenta del dispositivo móvil y luego al Departamento de Informática.

iii. En ambos casos debe existir una constancia policial del robo, sustracción o pérdida del dispositivo. La constancia debe ser entregada al patrocinador con copia al Departamento de Informática.

(l) Cualquier dato universitario almacenado en un dispositivo móvil sigue siendo propiedad de la Universidad y puede estar sujeto a investigación interna o divulgación por parte de la Universidad si hay un litigio en curso. Por lo tanto, quienes utilicen el dispositivo móvil deben ser conscientes de que existen situaciones en las que la Universidad puede estar obligada legalmente a revelarinformación que esté bajo su poder o control, y que no puede garantizar la protección completa de lainformación personal almacenada en los dispositivos de la Universidad.

4. Costos

(a) El titular del dispositivo móvil es responsable de todos los costos incurridos en su dispositivo móvil.

(b) Los costos derivados del uso excesivo de datos personales serán reembolsados por el titular del dispositivo móvil.

(c) La Universidad puede iniciar acciones para recuperar cualquier costo de uso personal del titular del dispositivo móvil.

5. Devolución, transferencia o eliminación

(a) Al cesar su empleo en la Universidad, el titular de un dispositivo móvil debe devolver todos los dispositivos móviles de la Universidad, completos con la tarjeta SIM y accesorios adicionales a su superior inmediato o al sub departamento de abastecimiento. El patrocinador del dispositivo móvil debe notificar al Departamento de Informática para que se tomen las medidas adecuadas con respecto a la cuenta móvil de la Universidad asociada con el dispositivo (s).

(b) Los dispositivos móviles y los números de teléfono de la Universidad siguen siendo propiedad de ésta. Las excepciones a esto deben ser aprobadas por la autoridad competente.

(c) Si un dispositivo móvil en el plan móvil de la Universidad se transfiere a otro titular de dispositivo móvil o centro de costos dentro de la Universidad, se debe informar al Departamento de Informática de los nuevos detalles.

(d) Todos los datos de un dispositivo móvil deben borrarse de forma segura antes de que el dispositivo se transfiera a otro miembro de la universidad.

(e) Los dispositivos móviles universitarios obsoletos o dañados deben devolverse al Departamento de Informática para su eliminación.

(f) Cuando cese la relación con la Universidad, todos los datos de la Universidad deberán eliminarse de forma segura de los dispositivos móviles externos.

(g) Todos los dispositivos móviles dados de baja o dañados no pueden ser eliminados en la basura, **deberán contactar a alguna de las empresas certificadas en recolección de desechos electrónicos**.

6. Incumplimiento

(a) El usuario del dispositivo puede enfrentar una acción disciplinaria y / o tenencia para undispositivo móvil puede ser revocada.

Control de versiones

Autor	**Fecha**	**Versión**	**Motivo**
Trends	08/01/2021	V00	Creación
UMCE – Trends	17/05/2021	V01	Revisión

D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

i. Propósito

El propósito de esta política es afirmar el compromiso de la Universidad con la gestión de la continuidad del negocio.
Mediante la adopción de las mejores prácticas de continuidad empresarial, la Universidad Metropolitana de Ciencias de la Educación, en adelante UMCE, logrará su objetivo de restaurar sus actividades críticas, administrativas, académicas y de investigación lo antes posible después de un evento disruptivo importante.
Esta Política de Gestión de la Continuidad del Negocio forma parte del Marco de Gestión de la Continuidad del Negocio de la UMCE, que está alineada con el estándar de Sistemas de Gestión de la Continuidad del Negocio ISO22301: 2012.

ii. Alcance

Esta política se aplica a toda la comunidad de la Universidad.
La Universidad no es responsable de desarrollar la política de gestión de la continuidad del negocio para sus entidades relacionadas. Los directorios/administradores de las entidades relacionadas serán responsables de establecer su propio marco y procesos de gestión de la continuidad del negocio.

iii. Definiciones

Continuidad del negocio: La capacidad de la organización, desde el servicio informático, para continuar la entrega de productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo.
Gestión de la continuidad del negocio: El proceso que identifica las amenazas potenciales a una organización y los impactos en las operaciones comerciales que esas amenazas, si se concretan, podrían causar, y que proporciona un marco para desarrollar la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de sus partes interesadas clave, la reputación. y actividades de la universidad.
Plan de Continuidad del Negocio. Procedimientos documentados que guían a la Universidad para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación después de una interrupción.
El proceso de analizar las actividades y el efecto que una interrupción del negocio podría tener sobre ellas.

iv. Contenido

La Universidad está comprometida a llevar a cabo sus actividades con el mayor respeto por la salud y seguridad de sus funcionarios, docentes, estudiantes y el público, y a proteger sus activos y reputación.
Por tanto, la UMCE debe:

- Establecer planes de continuidad servicio para garantizar la continuidad de sus actividades administrativas, académicas y de investigación clave.
- Revisar y actualizar anualmente los planes, incluido el mantenimiento periódico de los análisis de impacto de negocio (BIA) en los que se basan.
- Revisar los planes después de cualquier cambio estructural u operativo importante.
- Realizar ejercicios periódicos de validación del plan con fines de capacitación y evaluación del personal.
- Exigir a la administración que desarrolle, mantenga y delegue la planificación de la continuidad del negocio dentro de sus áreas de responsabilidad.
- Fomentar la participación activa de los funcionarios en asuntos de continuidad del negocio y asegurar que el personal clave pueda desempeñarse de manera competente durante un evento disruptivo importante.

Estas iniciativas se coordinarán con las actividades detalladas en la Universidad:

- Plan de gestión de emergencias, que proporciona una primera respuesta a una interrupción crítica.
- Plan de recuperación de desastres (DRP) de servicios de tecnología de la información, que se centra en la reanudación de datos y sistemas de tecnología de la información críticos.

Control de versiones

Autor	**Fecha**	**Versión**	**Motivo**
Trends	20/01/2021	V00	Creación
UMCE – Trends	14/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE PRIVACIDAD

i. Propósito

La Universidad Metropolitana de Ciencias de la Educación, en adelante, UMCE, se compromete a proteger la privacidad de quienes acceden a sus sitios web. El propósito de esta política es informar a quienes acceden a los sitios web de la UMCE sobre la recopilación y el uso de la información de identificación personal de sus usuarios.

ii. Alcance

Esta declaración de política de privacidad se aplica a todos los sistemas de información mecanizados o manuales de la UMCE.

iii. Definición de información de identificación personal

A los efectos de esta política, "información de identificación personal" significa cualquier información recopilada en línea que pueda servir para identificar a una persona, como, por ejemplo:

Nombre y apellido

Dirección física

Dirección de correo electrónico

Número de teléfono

Cedula de Identidad o pasaporte

Información de la tarjeta de crédito

Número de cuenta Bancaría

Cualquier combinación de información personal que pueda usarse para determinar la identidad

iv. Colección de información

La siguiente información puede recopilarse y retenerse automáticamente si mira o busca en nuestras páginas web o descarga información:

El dominio de Internet y la dirección de Protocolo de Internet (IP) de la computadora que está utilizando para acceder a nuestro sitio;
El tipo de navegador y sistema operativo utilizado para visitar nuestro sitio;
La fecha y hora en que accede a nuestro sitio; y qué

partes del sitio web visita.

Los datos recopilados sirven como parte de nuestro análisis estadístico sobre el uso de nuestros sitios web para que podamos diseñar mejor los servicios en línea y mejorar el acceso a ellos. No intentamos obtener información de identificación personal sobre usuarios individuales y asociarla con direcciones IP a menos que se indique explícitamente como parte de un servicio. La UMCE no utiliza la información recopilada automáticamente para determinar su información de identificación personal. La UMCE puede detectar direcciones IP de usuario para proporcionar información y servicios de usuario basados en la ubicación. La UMCE no mantiene ni recopila las direcciones IPde los usuarios, ni las divulga a terceros.
Excepto donde se especifique, no es necesario que proporcione información de identificación personal para visitar o descargar información de los sitios web de la universidad. A menos que elija que su información de identificación personal esté disponible para nosotros, la UMCE no recopila dicha información. La UMCE no usa ni coloca software espía en su computadora. Tenga en cuenta que algún servicio de los que presta la universidad puede solicitarle información de identificación personal para acceder a ellos.

v. Cómo utiliza la UMCE la información de identificación personal

Cualquier información de identificación personal que una persona proporcione a un sitio web de la universidad será utilizada únicamente por la UMCE, a menos que la información se designe expresamente como registro público en la misma página web.

vi. Seguridad y calidad de los datos

La UMCE está comprometida con la seguridad de los datos y la integridad de los datos de la información de identificación personal disponible o recopilada por los sitios web. La universidad ha tomado precauciones para proteger la información de identificación personal contra pérdida, mal uso o alteración. Todos los terceros autorizados responsables de esta información están comprometidos con los mismos principios y, por contrato, deben seguir las mismas políticas y pautas que la universidad para proteger esta información. Sin embargo, los visitantes deben tener en cuenta que, aunque existen protecciones, la universidad no puede garantizar que no se produzcan fallas de hardware, intrusiones no autorizadas u otros problemas técnicos.

vii. Sitios web no UMCE

Los visitantes pueden conectarse a varios sitios web desde las páginas web de la universidad. La UMCE no es responsable de las prácticas de privacidad o el contenido de sitios externos. Se recomienda a quienes visiten sitios externos que verifiquen la declaración de privacidad aplicable y tengan cuidado al proporcionar información de identificación personal sin una comprensión clara de cómo se utilizará la información.

viii. Cambios y versiones de la Política de privacidad

Esta política de privacidad se puede cambiar en cualquier momento; cualquier cambio se publicará en la página web. La información recopilada mientras una versión particular de esta política esté en vigor se manejará de acuerdo con esa versión. Si tiene preguntas, comentarios o inquietudes, comuníquese con el Departamento de Informática .

Control de versiones

Autor	Fecha	Versión	Motivo
UMCE - Trends	08/01/2021	V00	Creación
UMCE – Trends	14/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE REGISTRO DEL SERVIDOR

i. Propósito

Esta política sustenta un procedimiento de seguridad para las computadoras de la Universidad Metropolitana de las Ciencias de la Educación, en adelante UMCE, que tienen acceso a Internet. Esta política limita el acceso no solicitado a las computadoras desde fuera del campus al no permitir el acceso completo a los servidores a menos que lo autorice el Departamento de Informática .
Los servidores, con todos los servicios registrados, aumentan la probabilidad de ataque y compromiso del sistema. También permite a los atacantes instalar puertas traseras a las que se puede acceder desde Internet para un control continuo del sistema en caso de un compromiso.

ii. Alcance

Esta Política se aplica a toda la Universidad.

iii. Definiciones

DI – Departamento de Informática

Administrador del sistema: en el contexto de esta Política, la persona responsable de la administración y el mantenimiento de un servidor.

iv. Contenido

1. Política

(a) La Universidad ha implementado un procedimiento de seguridad para las computadoras de la Universidad que tienen acceso a Internet.

(i) No se permiten servidores de acceso completo.

(ii) Los administradores del sistema deben registrar sus servidores solo para los servicios de Internet relevantes.

(iii) Cualquier servidor de acceso completo debe ser autorizado por el Departamento de Informática.

(iv) Todos los servidores de la universidad tendrán bloqueado el servicio FTP y SFTP. La habilitación de estos servicios solo se podrá hacer bajo la supervisión del Departamento de Informática.

(v)Queda estrictamente prohibido y se debe bloquear o eliminar el servicio de escritorio remoto en cualquier servidor que se encuentre conectado a la red institucional sea propioo de terceros. De ser necesario se debe solicitar una conexión segura VPN para tales efectos al Departamento de Informática.

Control de versiones

Autor	Fecha	Versión	Motivo
Trends	20/01/2021	V00	Creación
UMCE – Trends	14/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DE USO DE INTERNET

i. Propósito

La Universidad Metropolitana de las Ciencias de la Educación, en adelante UMCE, proporciona equipos informáticos y acceso a Internet para que los funcionarios puedan realizar su trabajo para la Universidad, y permite un uso limitado para el uso que no está relacionado con el trabajo. El propósito de esta política es definir qué considera la Universidad como el uso apropiado de Internety cómo se administrará y monitoreará el acceso a Internet.

ii. Alcance

Esta política se aplica a todos los funcionarios, estudiantes, contratistas, visitas y empresas subsidiarias.

iii. Definiciones

Computadora: incluye cualquier dispositivo electrónico proporcionado por la Universidad, o conectado a sus redes, que sea capaz de acceder a Internet.

Uso de Internet: a los efectos de esta política, el uso de Internet incluye el acceso a sitios web, correo electrónico, redes peer to peer y uso compartido de datos.

Material inapropiado: es material que razonablemente podría describirse como inadecuado u ofensivo que viole las leyes chilenas, teniendo en cuenta la naturaleza del lugar de trabajo en particular e incluye material que es pornográfico o de otra manera objetable.

iv. Contenido

1. General

(a) El personal cuenta con instalaciones y equipos para acceder a Internet para actividades legítimas relacionadas con el trabajo.

b) El personal también puede utilizar las instalaciones de Internet de la Universidad para actividades no relacionadas con el trabajo, siempre que se lleve a cabo fuera del horario laboral habitual y esté limitado a tres horas por semana con no más de una hora por día. Esto incluye el uso personal de sitios de redes sociales como Facebook y Twitter.

(c) Los funcionarios y académicos tienen prohibido: crear, ver, acceder, intentar acceder, almacenar o mostrar material inapropiado, ya sea de forma electrónica o impresa.

(d) Si los funcionarios y/o académicos reciben un correo electrónico con contenido inapropiado, debe eliminarlo de inmediato y, cuando conozcan al remitente, notificar al remitente que no envíe dichos correos electrónicos, además, se debe notificar al Departamento de Informática.

(e) Si los funcionarios y/o académicos abren inadvertidamente un sitio web que contiene contenido inapropiado, debe salir del sitio web inmediatamente.

(f) Todo uso de conexiones peer to peer debe ser solo para negocios legítimos de la Universidad previa consulta al Departamento de Informática.

(g) Se acepta que pueden existir ocasiones en las que el personal académico requiera acceso a material inapropiado, o intercambios de dicho material entre colegas académicos, con fines de investigación o docencia u otro fin universitario legítimo. En esas circunstancias, el personal académico deberá poder justificar su acceso a satisfacción de la Universidad, o contar con la autorización escrita para tal acceso de su jefe directo o del Decano de su facultad.

2. Bloqueo del acceso a determinados sitios web

(a) La Universidad restringirá el acceso a ciertas categorías de sitios web y lo gestionará clasificando los sitios web en tres categorías:

(i) Sitios que están disponibles en todo momento, estos son todos los sitios excepto ii y iii a continuación.

(ii) Sitios bloqueados durante el horario normal de trabajo, que se define entre las 8:00 am y las 13:00 y las 14:00 a las 18:00, de lunes a viernes. Estas son categorías de sitios que es muy poco probable que tengan un uso laboral legítimo e incluyen:

- Sitios de subastas
- Sitios de citas
- Sitios de apuestas
- Sitios de juegos

(iii) Los sitios que contengan material pornográfico y / o censurable serán completamente bloqueados en la medida de lo posible.

(b) La vicerrectoría académica determinará los sitios que se bloquearán por recomendación de la jefatura del Departamento de Informática.

(c) Cualquier miembro del personal que tenga una necesidad legítima de acceder a los sitios de las categorías ii y iii puede solicitar acceso a su jefe directo o el decano de su facultad.

(d) El Departamento de Informática será responsable de administrar las restricciones de Internet y los departamentos, áreas, decanatos, facultades, jefaturas deberán asegurarse de que su acceso a Internet se filtre de acuerdo con esta Política y que cualquier software de administración de Internet esté instalado según lo determine el Departamento de Informática.

3. Seguimiento y ejecución

(a) Los equipos informáticos y el acceso a Internet se proporcionan con fines laborales y no para uso personal. En consecuencia, con la aprobación previa de la autoridad competente, la Universidad puede rastrear el uso, o examinar el contenido, de cualquier computadora que haya sido proporcionada por la Universidad, o que esté conectada a sus redes, en cualquier momento sin previo aviso al miembro del personal que usa la computadora. Esto incluye el acceso a correos electrónicos @umce.cl, cuentas dispuestas por la universidad, redes sociales, u otras comunicaciones electrónicas. Cuando dicho acceso sea apropiado por razones académicas, comerciales o de otro tipo genuinas, se debe obtener una exención del jefe directo de dicho funcionario.

(b) El Departamento de Informática es responsable de monitorear el uso de Internet y la administración de la red de acuerdo con esta política. Esto incluye:

(i) rastrear el uso e identificar contenidos inapropiados o riesgosos;

(ii) establecer un sistema para que el personal reconozca la política cuando inicie sesión por primera vez y que se repita anualmente.

(c) El Departamento de Informática notificará al jefe directo correspondiente y al departamento jurídico de cualquier sospecha de incumplimiento de esta política. Las infracciones de esta política pueden verse como una falta grave que podría resultar en la adopción de medidas disciplinarias.

Control de versiones

Autor	**Fecha**	**Versión**	**Motivo**

Trends	08/01/2021	V00	Creación
UMCE - Trends	14/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DEFINICIÓN CANALES DE COMUNICACIÓN

i. Propósito

Proporcionar un marco de comunicación que permita al Departamento de Informática, en adelante DI, la definición de canales de comunicación adecuados y la descripción de los tipos de comunicación para los que se puede utilizar cada uno de ellos.
Definir las responsabilidades de los usuarios con respecto a las comunicaciones formales de la Universidad.
Describir las mejores prácticas en la redacción y retención de comunicaciones de los usuarios.

ii. Alcance

En toda la universidad.

iii. Contenido

1. Canales y categorías de comunicación

a. Los canales de comunicación primarios suelen ser los medios más apropiados y / o fiables para contactar al DI:

- Correo electrónico
- El sitio web de Departamento de Informática.

b. Los canales de comunicación secundarios pueden ser apropiados para algunos mensajes:

- Teléfono
- Texto (servicio de mensajes cortos de teléfono móvil)
- Redes sociales (páginas oficiales de Facebook del Departamento, cuentas de Twitter, etc.)

c. Las categorías de comunicación son las siguientes:

i. Comunicaciones relacionadas con procesos administrativos y servicios de apoyo ii.

Comunicaciones de incidentes graves.

iii. Comunicaciones de solicitudes de servicio a usuarios o áreas.

iv. Comunicaciones generales no relacionadas con informática y posiblemente con un elemento social.

2. Canales de comunicación

a. La siguiente tabla está destinada a ayudar al personal a indicar los canales de comunicación adecuados para cada categoría de comunicación.

	Administración & Soporte	Incidente	Comunicaciones	General
Email	X	X	X	
Página web informática	X	X		X
Teléfono	X	X	X	
Mensaje telefónico	X	X	X	
Redes sociales informática (ej. Facebook/Twitter)				X
Video por Zoom	X	X		

b. Cualquier comunicación específica debe realizarse a través de un canal o canales apropiados, pero no es necesario que se realice a través de todos los canales.

c. Se debe tener en cuenta el hecho de que algunas comunicaciones se clasificarán como registros y deberán conservarse según los requisitos de mantenimiento de registros para futuros análisis.

d. Las comunicaciones por correo electrónico deben dirigirse a las direcciones de correo electrónico proporcionadas por el D.I. Sin embargo, cuando, con respecto a un determinado asunto, un usuario:

i. Inició un intercambio de correo electrónico desde una dirección de correo electrónico que no es de usuario UMCE; o

ii. Proporcionó una dirección de correo electrónico no UMCE para un propósito específico (por ejemplo, una solicitud de préstamos); o

iii. Respondió a un correo electrónico de la Universidad desde una dirección de correo electrónico que no era del dominio UMCE, es aceptable utilizar esa dirección de correo electrónico en relación con ese asunto particular.

e. Las redes sociales deben usarse con moderación para las comunicaciones relacionadas con la solicitud de servicios o reporte de incidentes..

3. Redacción y retención de comunicaciones

Sujeto a las limitaciones del canal de comunicación utilizado, todas las comunicaciones del Departamento de Informática hacia y desde la Universidad deben:

i. Ser claras, cortés, precisas, apropiadas, oportunas y sin jerga; ii.

contener la fecha; iii. contener el nombre del autor y el cargo o el área

responsable;

iv. contener los datos de contacto de la persona a quien se deben dirigir las consultas sobre la comunicación, si no es el autor;

v. ser consistente con las políticas y procedimientos de la Universidad;

4. Responsabilidades

a. El personal de comunicaciones, actuando como el Equipo de Comunicaciones, es responsable de las comunicaciones durante un estado de necesidad del Campus, con la excepción de los anuncios del rector, vicerrector o delegado, según el Plan de Comunicaciones de Emergencia.

b. Los miembros del personal y las unidades que prestan servicios específicos son responsables de:

i. Comunicarse con los usuarios, individualmente y en grupo, sobre procesos e información relacionados con un servicio específico;

ii. Comunicarse de forma individual con los usuarios que están comprometidos con un servicio.

c. El Departamento de Informática (DI) solo responderá a correos institucionales. Si un usuario envía un correo desde una dirección de correo electrónico que no sea una dirección asignada por la Universidad, o proporciona una dirección de correo electrónico alternativa para un propósito específico, informática no atenderá ese requerimiento a menos que esté plenamente identificado y sea por temas puntuales en forma temporal. Por ejemplo, una consultoría externa.

d. La Universidad no se hace responsable de las comunicaciones no recibidas por los usuarios de una dirección de correo electrónico alternativa.

e. La recepción y posterior asignación de los requerimientos de los usuarios hacia informática será administrada y controlada por una persona designada por informática para tales tareas con el fin de eliminar el tráfico innecesario de mensajes, correos, llamadas, etc. al personal de informática. Esto permitirá hacer seguimientos a las solicitudes.

f. Todas las solicitudes quedaran registradas en el sistema de gestión de incidencias (soporte.umce.cl) donde el usuario podrá hacer el seguimiento de su solicitud y revisar el estado de ésta.

Control de versiones

Autor	Fecha	Versión	Motivo
Trends	20/01/2021	V00	Creación
UMCE – Trends	14/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DERECHOS DE AUTOR DEL SOFTWARE

i. Objetivo:

Los miembros de la universidad deben conocer las disposiciones de la Ley de derechos de autor (Ley N° 17.336 sobre Propiedad Intelectual) y sus modificaciones, la aplicación de estas disposiciones al uso de software comprado o con licencia de proveedores externos. Esta política se ha desarrollado en un esfuerzo por aumentar la conciencia y fomentar el cumplimiento de estas disposiciones.

ii. Alcance

Esta política se aplica a toda la comunidad universitaria, contratistas, invitados, consultores, empleados temporales de la Universidad y cualquier otro usuario que sea responsable de los recursos de tecnología de la información de la Universidad o tenga acceso a ellos.

iii. Política:

Los estudiantes de todos los cursos que hacen un uso extensivo de programas con derechos de autor deben ser conscientes de los problemas legales, éticos y prácticos causados por la pirateríade software.
La ley de derechos de autor regula la copia y el uso de programas de computadora que tienen derechos de autor. Sin embargo, el acuerdo de licencia particular aplicable al software puede ser más restrictivo que las leyes de derechos de autor. En ese caso, el usuario del programa debe cumplir con las disposiciones del acuerdo de licencia aplicable, así como con las disposiciones de laley.
El Departamento de Informática es quien supervisara el cumplimiento de esta política.

iv. Definiciones:

Universidad: se refiere a la Universidad Metropolitana de Ciencias de la Educación, en adelante UMCE en su conjunto e incluye todas las unidades.

v. Procedimiento:

A. Requisitos de la ley de derechos de autor.

1. La ley de derechos de autor establece que no constituye una infracción que el propietario dé una copia de un programa informático realice o autorice la realización de otra copia o adaptación de ese programa siempre que:

    a. Que esa nueva copia o adaptación se crea como un paso esencial en la utilización del programa de computadora junto con una máquina y que no se usa de otra manera, o
    b. Que esa nueva copia y adaptación es únicamente para fines de archivo y que todas las copias de archivo se destruyen en caso de que la posesión continuada delprograma de computadora deje de ser legítima.

2. Si el cumplimiento de las disposiciones anteriores no es aceptable, es decir, si el usuario desea hacer copias adicionales, el usuario debe obtener el permiso previo por escrito de la compañía que posee los derechos de autor del software para usar o copiar los programas de una manera diferente a lo previsto por la ley o los términos del contrato de licencia.

B. Licencias de software

1. El inicio de las negociaciones del contrato debe ser aprobado por la jefatura del Departamento de Informática.
2. Cada unidad académica o administrativa de la Universidad es responsable de establecer prácticas que harán cumplir esta política. Lo siguiente es apropiado para publicar un aviso cerca de computadoras y / o terminales de computadora:
    i. Los programas de computadora pueden estar protegidos por leyes de derechos de autor o acuerdos de licencia.
    ii. Está prohibido copiar dichos programas sin el permiso escrito correspondiente.

C. Infracciones

1. Todas las violaciones conocidas y / o sospechadas deben informarse al Departamento de Informática. Todas estas denuncias de mal uso serán investigadas por la Contraloría Interna de la Universidad con el apoyo técnico del Departamento de Informática.
2. El conocimiento de las violaciones de la política se abordará mediante políticas y procedimientos disciplinarios.

Control de versiones

Autor	**Fecha**	**Versión**	**Motivo**
Trends	08/01/2020	V00	Creación
UMCE – Trends	07/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA PARA LA DESTRUCCIÓN Y ELIMINACIÓN DE EQUIPOS Y DATOS ELECTRÓNICOS

El propósito de esta política es ayudar a las escuelas, institutos, departamentos y otras unidades de la Universidad Metropolitana de Ciencias de la Educación, en adelante UMCE, a proteger la información confidencial de la divulgación no autorizada, así como a cumplir con los acuerdos de licencia de software, el estado, las leyes y regulaciones de seguridad y privacidad de datos que la afectan.

i. Alcance

Están cubiertos por esta política todas las computadoras y dispositivos de almacenamiento digital, incluidos, entre otros, estaciones de trabajo de escritorio, servidores, computadoras portátiles, dispositivos móviles, impresoras y discos duros de computadoras de mano; discos duros externos; y todos los dispositivos de almacenamiento externo, como discos, SAN, medios ópticos (por ejemplo, DVD, CD), medios magnéticos (por ejemplo, cintas, disquetes) y medios electrónicos no volátiles (por ejemplo, tarjetas de memoria, pendrives).

ii. Política

Los programas de software con licencia, los datos institucionales / comerciales, los datos de identificación personal o identificables y / o los datos no públicos deben borrarse y / o destruirse de manera confiable de cualquier dispositivo electrónico antes de que el dispositivo se transfiera fuera del control de la Universidad o se borre antes de ser transferido a otro departamento o particular. No borrar los datos de manera adecuada de forma que sean irrecuperables puede representar un riesgo significativo para la Universidad, ya que los datos a menudo se pueden recuperar fácilmente con herramientas disponibles en internet. En todos los casos, se debe seguir esta política al tomar esas decisiones.

1. **Eliminación de registros que contienen información de identificación personal u otros datos confidenciales**

    1.1. Primero, se debe evaluar cada dispositivo para determinar si el dispositivo debe borrarse o si los datos del dispositivo deben conservarse y transferirse a otro lugar dentro de la Universidad.

    1.2. Ningún registro que contenga información de identificación personal, incluidos, entre otros, datos de riesgo bajo, riesgo moderado y alto riesgo (consulte la Política de clasificación de riesgos del sistema y datos electrónicos de la UMCE) deberá desecharse a menos que se lleve a cabo la siguiente limpieza:

- destruir la información de identificación personal contenida en el registro; o
- modificar el registro para hacer ilegible la información de identificación personal

    1.3. Aunque no es obligatorio, se recomienda que la información electrónica disponible públicamente también se elimine del dispositivo.

    1.4. Los datos que deben conservarse y transferirse a un dispositivo nuevo u otro deben realizarse en consulta con el Departamento de Informática.

    1.5. El software con licencia y los datos institucionales considerados propiedad de la UMCE deben eliminarse antes de transferir el equipo de la Universidad.

    1.6. La UMCE debe retener el software comprado y / o implementado con licencia (por ejemplo, Microsoft Office, Adobe Creative, otros programas) para una posible reinstalación.

2. **Metodología de borrado**

    2.1. Eliminar archivos de un dispositivo es un primer paso, pero no elimina los datos. Los datos que se han "eliminado" sin utilizar uno de los métodos que se enumeran a continuación simplemente se pueden "recuperar".

    2.2. Si bien es más importante salvaguardar datos universitarios no públicos y / o personalmente identificados o identificables, a menudo es difícil separar clasificaciones de datos específicas o determinar de manera concluyente que los remanentes de datos no públicos no son recuperables. Por lo tanto, es más conveniente y rentable purgar todos los datos no públicos antes de reutilizarlos o eliminarlos, en lugar de intentar borrar de forma selectiva los datos.

    2.3. Algunos métodos de destrucción de datos son más complicados, requieren más tiempo o requieren más recursos que otros. La selección debe basarse en la sensibilidad subyacente de los datos que se destruyen.

2.3.1 Borrar / sobrescribir

El borrado por sobre escritura es un método aceptable para borrar datos que no son confidenciales o requieren protección. Se deben realizar varias pasadas con patrones de sobre escritura aleatorios,

no solo con ceros u otro carácter único. Se requiere un mínimo de tres (3) sobre escrituras; Se recomienda una sobre escritura adicional dependiendo de la sensibilidad de los datos que se borrarán. Los productos que se enumeran a continuación son gratuitos y pueden sobrescribir los sistemas operativos Microsoft y Unix.

- Active @ Kill Disk (Estándar del Departamento de Defensa)
- Eliminación segura de disco duro DBAN
- Borrador seguro de Windows
- Borrado seguro o Vaciado seguro de la papelera en Mac OS X 10.6.8 o posterior (3, 5 o 7 pasadas)

2.3.2 Desmagnetización

La desmagnetización es una forma en que la carga magnética de un objeto se restablece a un estado magnéticamente neutro, borrando de hecho todos los datos previamente escritos en el disco duro o la cinta.

2.3.3 Destrucción

En los casos en los que los datos no se pueden sobrescribir o cuando no es posible desmagnetizar, los discos duros deben destruirse físicamente. Para las unidades que están defectuosas, muertas o que no responden lo suficiente como para no completar al menos un mínimo de tres sobre escrituras, se requiere destrucción física.

2.4. Pueden surgir situaciones especiales que impidan o dificulten excesivamente el cumplimiento de esta política. Para estas situaciones o desafíos únicos, comuníquese con el Departamento de Informática.

2.5. Tenga en cuenta que una variedad de factores puede afectar la efectividad y la integridad de la operación de sobre escritura. No se recomienda transferir o reutilizar el dispositivo fuera de la UMCE a menos que el borrado se pueda validar por completo.

2.6. El proceso de destrucción física deberá ser certificado y documentado por un ministro de fe del departamento jurídico, en caso contrario, por un notario público.

2.7. Todo dispositivo dañado, dado de baja o destruido, no podrá ser desechado en la basura requiriendo para ello el uso de empresas certificadas por el Ministerio del Medio Ambiente para el retiro y posterior disposición de dichos elementos.

3. Proceso de eliminación

3.1. Ninguna computadora o dispositivo de almacenamiento digital que sea objeto de eliminación o baja, puede dejar la posesión o tenencia de la Universidad sin someterse a la metodología de borrado descrita.

3.2. Se requiere documentación, para posibles propósitos de auditoría, que acredite el borrado del software con licencia y los datos institucionales para completar la transferencia tanto dentro como fuera de la Universidad, incluidos los dispositivos para el intercambio que deben reemplazarse como parte de una garantía o contrato de reparación. La documentación debe conservarse de forma segura en el Departamento de Informática.

3.3. Cada garantía o contrato de reparación debe contener una declaración sobre el borrado de los datos del disco duro, incluida una descripción del procedimiento del proveedor para el borrado. Si el reemplazo es necesario como parte de un contrato de garantía o reparación y el borrado del disco duro no se puede lograr por razones técnicas, el proveedor que recibe el dispositivo debe tener un acuerdo contractual para permitir que la UMCE retenga el disco duro y / o un contrato de confidencialidad y acuerdo de no divulgación vigente con la UMCE. Si ninguno de los acuerdos está vigente, antes de devolver el dispositivo al proveedor, UMCE debe retirar el disco duro y asegurarse de su destrucción.

3.4. El Departamento de Informática deberá especificar la persona técnica responsable del proceso de borrado y eliminación en esa unidad, departamento, facultad o ubicación.

3.5. Se debe crear un registro de los dispositivos que han sido borrados a modo de evidencia de la limpieza y protección de los datos de la UMCE. Se debe incluir información que incluya, entre otros, la ubicación del dispositivo, la fecha de borrado, el nombre de las personas responsables, la disposición después del borrado, nombre del técnico que ejecuto el borrado. El procedimiento debe ser aplicado en cualquier área usuaria de los serviciosque presta el Departamento de Informática.

3.6. La persona responsable del proceso de borrado y eliminación debe evaluar el dispositivo y asegurarse de que los datos se hayan eliminado de manera adecuada ycompleta del disco duro antes de su eliminación o reinstalación.

3.7. La persona responsable del proceso de borrado y eliminación en la unidad debe documentar que el proceso de borrado y eliminación se completó y conservar de forma segura la documentación. (Ver punto 3.2).

3.8. Una unidad que solicite retener el dispositivo más allá del período de renovación asume la responsabilidad del dispositivo.

3.9. El dispositivo se puede reutilizar dentro o fuera de la Universidad una vez que se haya completado el proceso de borrado / sobre escritura y cuente con la certificación documentada del borrado.

iii. Definiciones

Borrado: Proceso mediante el cual los datos (información, registros) se eliminan irreversiblemente del dispositivo o se destruyen permanentemente.

Borrado / sobreescritura binaria: El software escribe ceros y unos aleatorios sobre los datos existentes.

Clasificación de datos: La Política de clasificación de riesgos de sistemas y datos electrónicos está destinada a describir la confidencialidad de los datos en cuestión y no tiene en cuenta los requisitos de integridad o disponibilidad en su calificación. La clasificación de los datos puede depender del contexto en el que se utilizan los datos. Tenga en cuenta que, si un dato encaja en más de una categoría, se considera que es la más alta de esas clases.

Control de versiones

Autor	Fecha	Versión	Motivo
Trends	21/01/2020	V00	Creación
UMCE – Trends	19/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA DEL SERVIDOR DE CORREO ELECTRÓNICO

i. Propósito

El propósito de esta Política es definir las especificaciones / requisitos que deben cumplir todos los servidores de correo electrónico.

ii. Alcance

Esta Política se aplica a toda la Universidad.

iii. Contenido

1. Política

Para reducir las infecciones de virus en la universidad y detener la retransmisión de correo electrónico inapropiado, todos los servidores de correo electrónico existentes deben retransmitir el correo electrónico externo, por medio de los buzones de correo centrales y también deben utilizar esos sistemas para escanear el correo electrónico entrante.
Si se requiere un servidor de correo electrónico adicional, el jefe del departamento, área o facultad que desee configurar el servidor debe contactar a la jefatura del Departamento de Informática para explicar la necesidad del servidor de correo electrónico.
Los administradores de todos los servidores de correo electrónico que utilizan los buzones de correo deben implementar políticas anti-relay adecuadas para sus sistemas. Esto variará para cada servidor, pero debe garantizar que los usuarios no autorizados no transmitan el correo electrónico a través del servidor primario. Esto es para garantizar la integridad general del sistema de correo electrónico de la Universidad.
Solo los buzones de correo centrales podrán comunicarse fuera del campus para recibir correo electrónico en el puerto smtp (puerto 25).

Control de versiones

Autor	**Fecha**	**Versión**	**Motivo**
Trends	08/01/2020	V00	Creación
UMCE – Trends	19/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

POLÍTICA SOBRE EL USO DE LAS COMPUTADORAS Y LOS DATOS DE LA UMCE

i. Objeto de esta política

La Universidad Metropolitana de Ciencias de la Educación (en adelante UMCE) es una Institución de Educación Superior sin fines de lucro, y sus instalaciones, incluidos los recursos informáticos y de datos, se utilizarán para promover sus fines educativos, de investigación y de servicio. Cada vez se realizan más actividades universitarias utilizando computadoras y comunicaciones electrónicas, con una mayor comodidad y accesibilidad desde y hacia todas partes del mundo. Al mismo tiempo, el entorno interconectado actual intensifica los riesgos y las amenazas del acceso no autorizado a las computadoras, la divulgación inadvertida de datos sensibles y la destrucción inesperada de información esencial, lo que tiene como resultado consecuencias potencialmente graves para las personas y las instituciones. Los miembros de la comunidad universitaria interactúan con un amplio espectro de datos sensibles por numerosas razones. La evolución de los ciber ataques, robos de información y fraudes electrónicos requieren que las organizaciones y las personas protejan la información confidencial. Con la informática tan ampliamente distribuida en toda la UMCE, la responsabilidad de proteger las computadoras y los recursos de datos se extiende a todos los miembros de la comunidad universitaria.

ii. Alcance

Esta política se aplica a los miembros de la comunidad universitaria que utilizan los recursos informáticos y de datos de la UMCE y / o que tienen acceso a datos confidenciales enviados, transmitidos, vistos, recibidos o almacenados en estos recursos.

iii. Definiciones de política

Afiliados se refiere a personas que tienen relaciones contractuales o de otro tipo con la Universidad y que no son funcionarios, docentes o estudiantes.

La autorización en este contexto significa otorgar permiso a una persona identificada para usar una computadora o un recurso de datos. La aceptación de la autorización para usar los recursos informáticos y de datos de la UMCE establece una obligación por parte del individuo de usar esos recursos de manera responsable.

Los recursos informáticos y de datos incluyen computadoras y dispositivos informáticos, tanto alámbricos como inalámbricos; acceso a la informática, aplicaciones y bases de datos (incluidas contraseñas); servicios de software, hardware, informática y correo electrónico; y cuentas informáticas asociadas. Las computadoras y los dispositivos informáticos incluyen, entre otros, computadoras de escritorio o portátiles, teléfonos inteligentes y teléfonos celulares, unidades de memoria flash USB o dispositivos similares, y todos los demás dispositivos móviles en los que se pueden enviar, transmitir, ver, recibir o almacenar datos de alto riesgo(sensibles).

Los miembros de la comunidad universitaria se refieren a funcionarios, docentes y estudiantes de tiempo completo y parcial.

Los datos confidenciales incluyen, pero no se limitan a, información sobre estudiantes potenciales, actuales y anteriores, clientes de instalaciones y servicios que preste la universidad a lacomunidad; también información sobre investigación, negocios universitarios, finanzas, operaciones, y contraseñas. Las políticas y procedimientos de la Universidad regulan el manejo y la utilización de muchos tipos diferentes de datos confidenciales. Consulte la Política de clasificación de riesgos de sistemas y datos electrónicos de la Universidad.

iv. Política universitaria

La UMCE espera que los miembros de la comunidad universitaria empleen medidas de seguridad administrativas, técnicas y físicas razonables y apropiadas para proteger la computadora, los recursos de datos que utilizan y los datos confidenciales almacenados en estos recursos. El acceso a la computadora y los recursos de datos (incluidos software, hardware, computadora y servicios de correo electrónico) son privilegios que se otorgan a los miembros de la comunidad universitaria, y deben ejercerse de conformidad con todas las políticas y procedimientos aplicables de la UMCE y todas las leyes vigentes. El acceso a los recursos informáticos y de datos está limitado a personas autorizadas y solo para fines aprobados. Los propósitos aprobados son aquellos consistentes con los objetivos generales de instrucción y de investigación de la Universidad y la relación de lapersona con la Universidad. La autorización para utilizar estos recursos es otorgada por personas designadas en la Universidad a quienes se les ha confiado la responsabilidad general y la gestiónde los datos y sistemas relacionados. La aceptación de la autorización para usar los recursos informáticos y de datos establece una obligación por parte del individuo de usar estos recursos de manera responsable, según se define a continuación.

Esta política no constituye un contrato de ningún tipo, incluyendo, entre otros, un contrato de trabajo. La Universidad se reserva el derecho de modificar esta política sin previo aviso y a su discreción. La versión actual de esta política está publicada en el sitio web de Informática de la UMCE (informática.umce.cl/políticas).

v. Requisitos de la política

A. La aceptación de la autorización para utilizar los recursos informáticos y de datos de la UMCE establece la obligación de:

1. Utilizar los computadores y datos con propósitos educativos, de investigación y de servicio de la UMCE de manera que cumpla con esta y otras políticas y procedimientos aplicables y con todas las leyes y regulaciones aplicables;
2. No usar su cuenta para ningún propósito comercial;
3. Comportarse con respeto hacia otros miembros de la comunidad de la UMCE y de la comunidad en general en Internet;
4. Tomar medidas razonables para garantizar que cualquier computadora que se utilice para acceder a los recursos de la UMCE, ya sea que esté ubicada en un campus de la UMCE o enotro lugar, sea segura, esté libre de virus y no se vea comprometida;
5. Proteger la confidencialidad, seguridad, integridad y capacidad de recuperación de todos los recursos informáticos y de datos y tomar las medidas razonables y apropiadas para proteger estos recursos del uso indebido o no autorizado, incluido el uso por parte de terceros;
6. Utilizar aplicaciones que se ajusten a las políticas, pautas de privacidad y seguridad de la UMCE;
7. Abstenerse de actividades que interfieran con la capacidad de otros para usar recursos informáticos y de datos; y
8. Conocer y cumplir con otras políticas, procedimientos y reglas relevantes de la Universidad, las leyes y regulaciones aplicables; en todos los casos se debe seguir la norma más estricta.

B. Esta obligación se aplica independientemente de:

1. Donde se encuentre la computadora utilizada para acceder a los recursos informáticos y de datos sea en una oficina, aula, espacio público o laboratorio de la UMCE, o en casa o en cualquier otro lugar fuera de la Universidad;

2. Quién es el propietario del dispositivo utilizado para acceder o almacenar los datos confidenciales; o

3. La forma o manera en que se almacenan o transmiten los datos confidenciales, incluidos, entre otros, archivos locales, archivos compartidos, archivos en medios extraíbles como discos DVD y unidades removibles, base de datos, fax, impresora, fotocopiadora, red, teléfono, correo electrónico o correo de voz.

C. El acceso y uso, o permitir el acceso y uso, de recursos informáticos y de datos, incluidos los servicios de correo electrónico, por cualquier persona que no sea lo permitido por la UMCE está estrictamente prohibido y puede someter al infractor a sanciones legales y/o civiles, así como procedimientos disciplinarios iniciados por la universidad.

D. El uso de algunos recursos informáticos y de datos de la UMCE puede estar regido por políticas y procedimientos adicionales de la Universidad, la escuela, el departamento o área. Cualquier persona autorizada a utilizar estos recursos es responsable de cumplir con dichas políticas y procedimientos.

E. Para salvaguardar la seguridad y eficiencia de los recursos informáticos y de datos, los sistemas informáticos de la UMCE son monitoreados de manera rutinaria para verificar la integridad y operación del sistema por parte del personal autorizado de la Universidad. Los recursos informáticos y de datos proporcionados por la universidad **son propiedad de la UMCE y no propiedad personal del individuo.**

F. Las personas designadas en la Universidad a quienes se ha confiado la responsabilidadgeneral y la administración de los recursos informáticos, de datos, datos confidenciales y sistemas relacionados tienen autoridad para tomar decisiones para autorizar el acceso y el uso de esos recursos y sistemas;

1. Estas personas en la Universidad pertenecen al Departamento de Informática, principalmente a su jefatura.

2. Estas personas en la Universidad tienen la responsabilidad del desarrollo, implementación y mantenimiento de políticas y procedimientos relacionados con la autorización del acceso a los datos confidenciales en uso de forma electrónica en UMCE y de manejar esos datos apropiadamente. Dichos individuos pueden delegar responsabilidades según lo consideren apropiado en áreas funcionales específicas.

3. Estas personas en la Universidad pueden tener estándares más estrictos para el uso, almacenamiento y transmisión de los datos que manejan que los establecidos en esta política; se debe seguir el estándar más estricto. Se espera que las personas autorizadas a utilizar los datos conozcan las políticas vigentes y las cumplan.

4. El acceso a los datos confidenciales se otorgará solo sobre la base de "según sea necesario / mínimo necesario".

G. La jefatura de informática de la Universidad es responsable de las revisiones periódicas de las políticas y procedimientos de seguridad de la Universidad relacionados con los recursos informáticos, datos y datos confidenciales, que se revisarán según sea necesario y se publicaránsus respectivas actualizaciones. Las versiones actuales de las políticas de la Universidad relacionadas con los recursos informáticos, datos y datos confidenciales se mantienen en el sitioweb de informática de la UMCE (informática.umce.cl/políticas).

H. Los infractores de esta política pueden estar sujetos a medidas disciplinarias, incluyendo la destitución o, en el caso de estudiantes, suspensión o expulsión de la Universidad. Cualquiera que sepa o tenga motivos para creer que otra persona ha violado esta política deberá informar el asunto de inmediato a su jefatura directa. Cualquier intento de tomar represalias contra una persona por informar una infracción se considerará en sí mismo una infracción de la política y puede resultar en una acción disciplinaria que puede incluir el término del contrato con la Universidad. La Contraloría Interna realizará la Investigación Sumaria o Sumario Administrativo según sea pertinente, para determinar la responsabilidad administrativa, académica o estudiantil correspondiente, actuará con el apoyo técnico del Departamento de Informática el que además tomará medidas para remediar o corregir la situación mientras se realiza el procedimiento de investigación.

vi. Especificaciones

A. Seguridad informática de la UMCE

Los controles de seguridad informática se basan en que los datos de una máquina / dispositivo individual influyen en la clasificación de esa máquina / dispositivo y, a su vez, en la estrategia de seguridad para la defensa contra el acceso no autorizado.

1. Protección de computadoras para uso individual

Esta sección describe las medidas para proteger las computadoras que suelen utilizar las personas en actividades relacionadas con la UMCE para acceder a otros recursos de la Universidad, como la intranet. Tal como se utiliza en estas especificaciones operativas, las "computadoras" incluyen, entre otras, computadoras de escritorio o portátiles, teléfonos inteligentes y teléfonos celulares, unidades de memoria flash USB o dispositivos similares.

a. Seguridad física

i. No dar acceso físico a las computadoras a personas no autorizadas.

ii. Tomar las precauciones necesarias para evitar robos y daños.

iii. Siempre que sea posible, posicionar los monitores para evitar que los visitantes o transeúntes los vean ocasionalmente.

b. Sistema de seguridad

i. Instale software antivirus y mantenga actualizadas las definiciones de virus.

ii. Instale parches de software y sistema operativo y tome otras medidas recomendadas para mitigar las vulnerabilidades conocidas de la computadora de manera oportuna.

iii. Utilice únicamente software aprobado por la UMCE; no descargue software no autorizado.

iv. Utilice un protector de pantalla de bloqueo u otro mecanismo para evitar el uso noautorizado de la computadora.

v. No deje su computadora desatendida sin bloquearla o cerrar la sesión.

vi. No instale ni utilice software para compartir archivos peer to peer; Estos programas generalmente permiten el acceso remoto no autorizado sin contraseña al contenido de la computadora.

vii. No instale ni ejecute software que requiera una licencia sin esa licencia. Respete los acuerdos de licencia y no infrinja los derechos de autor de otros.

viii. Responda con prontitud a los avisos del personal autorizado de la Universidad de que se han detectado vulnerabilidades en el sistema de su computadora.

ix. Tenga especial cuidado de proteger su información de acceso a la UMCE (por ejemplo, inicios de sesión, contraseñas) en las computadoras de su hogar contra el uso no autorizado por otros.

X. No instale aplicaciones de terceros no seguras que puedan enviar malware a un dispositivo personal en el que pueda tener datos de alto riesgo, poniendo así a la UMCE en riesgo de violación.

C. Contraseñas

i. Siempre que sea posible, proteja todas las cuentas de computadora con contraseñas y use contraseñas para proteger todos los archivos compartidos.

ii. Utilice contraseñas seguras. Las contraseñas seguras constan de al menos ocho (8) caracteres. No deben ser palabras de diccionario ni fáciles de adivinar. Deben incluir al menos tres (3) de las siguientes cuatro (4) características en cualquier orden: letras mayúsculas, minúsculas, números y símbolos. **Revise la política de contraseñas de la UMCE.**

iii. Cambie las contraseñas periódicamente. Evite reutilizar una contraseña durante al menos varias iteraciones de cambio. Si tiene varias cuentas, evite usar la misma contraseña

para esas cuentas. Puede encontrar información adicional sobre contraseñas en la política de contraseñas de la UMCE.

iv. No guarde las contraseñas en texto sin formato en un archivo de computadora o en papel a la vista. Las contraseñas no deben enviarse por correo electrónico ni proporcionarse verbalmente por teléfono. Si debe comunicar la información de acceso a la cuenta para garantizar la continuidad del negocio, debe comunicarla de manera segura. Los directivos deben asegurarse de que las oficinas tengan planes de acceso a archivos y datos para la continuidad del negocio (organización).

v. Mantenga una copia segura de sus contraseñas disponible para acceso de emergencia. Cifre cualquier archivo de computadora que contenga contraseñas. Mantenga cualquierarchivo escrito de contraseñas en un lugar físicamente seguro, preferiblemente separado de la computadora o aplicación que protegen.

vi. Las contraseñas de sitios web confidenciales o cuentas de correo electrónico no deben guardarse en la computadora.

vii. Siempre que sea posible, no configure programas para almacenar contraseñas automáticamente.

viii. Cierre los navegadores web, los programas de correo electrónico u otras aplicaciones que puedan almacenar contraseñas temporalmente cuando no estén en uso.

d. Acceso remoto

i. Cualquier computadora remota que se use para acceder a los recursos de la UMCE debe cumplir con estas especificaciones y puede estar sujeta a restricciones adicionales específicas de recursos.

ii. Si no mantiene o controla la computadora remota, no la use para acceder o transmitir datos confidenciales. Puede que se permita el acceso a datos no sensibles. Consulte con el departamento responsable o un supervisor para obtener orientación.

iii. Utilice el software y los servicios de acceso remoto con precaución. Preste especial atención a la configuración del software, hardware y servicios de acceso remoto para asegurarse de que no presenten un riesgo de seguridad para su computadora o la universidad. Consulte con el área de seguridad del Departamento de Informática de la UMCEpara obtener orientación sobre cómo elegir, configurar y operar tecnologías de accesoremoto.

iv. Asegúrese de que su computadora no esté configurada para permitir el acceso no autorizado a la red de la UMCE por parte de otros dispositivos. Los accesos especiales, como el acceso inalámbrico, el acceso a los servicios RAS (Servidor de acceso remoto) y las conexiones de red compartidas, deben ser autorizadas por el Departamento de Informática de la universidad.

2. Protección de las computadoras utilizadas por varias personas

Esta sección cubre medidas adicionales para proteger las computadoras utilizadas por varias personas. Se aplican todas las especificaciones operativas establecidas anteriormente, así como las siguientes medidas adicionales para salvaguardar dichos equipos.

a. Asegure todas las cuentas de las computadoras con contraseñas.

b. Entregar cuentas solo a personas autorizadas; proporcionar inicios de sesión individuales. Si comparte una computadora con otras personas, tome las precauciones adecuadas para salvaguardar los datos confidenciales a los que otras personas pueden no estar autorizados a acceder y, cuando sea posible, cree cuentas separadas para cada persona autorizada a usar la computadora, estableciendo los permisos adecuados.

c. Siempre que sea posible, haga cumplir el uso de contraseñas seguras y cambios periódicos de contraseña.

d. Haga todo lo posible por mantener los registros de la computadora(logs) y revíselos con regularidad.

e. Utilice las mejores prácticas para administrar la computadora en particular.

3. Continuidad comercial

Tome las medidas razonables para asegurarse de que, en caso de emergencia, otra persona autorizada pueda acceder a la computadora que utiliza para brindar continuidad a las funciones realizadas en ella y a través de ella. Los intereses de la Universidad deben equilibrarse con la protección y la privacidad de los datos. Existen numerosos métodos disponibles para garantizar la responsabilidad compartida de los datos y los sistemas en lugar de compartir contraseñas. Para obtener ayuda, comuníquese con el área de seguridad del Departamento de Informática.

4. Compras

Analice el cumplimiento de las políticas y procedimientos aplicables de la universidad como parte del proceso de compra. Las computadoras y el software adquiridos para su uso con los recursos informáticos y datos deben cumplir con estas especificaciones.

5. Licencias de software

Los usuarios de software deben usar e instalar solo software con la licencia adecuada en las computadoras y la red de la UMCE.

a. La duplicación, distribución, descarga, intercambio, venta o instalación no autorizada de software y documentación relacionada o el uso de software sin licencia y documentación relacionada constituye una violación del contrato de licencia de software y de la política de la Universidad.

b. Cada escuela, departamento u otra unidad es responsable de garantizar que el software utilizado en sus computadoras tenga la licencia adecuada, de cumplir con los términos y condiciones de esas licencias de software y de mantener la documentación adecuada de esas licencias de software.

C. Tras la desvinculación de la UMCE, todo el software propiedad de la Universidad, incluido todo el software con licencia de la universidad, debe eliminarse de las computadoras que no pertenecen a la UMCE. Esto incluye dispositivos móviles, portátiles y equipos domésticos. Si tiene software en la computadora de su oficina que le permite instalar una segunda copia en la computadora de su hogar, elimine esa segunda copia.

6. Eliminación o reutilización de equipos

a. Antes de desechar o volver a utilizar el hardware, cumpla con las pautas de desecho de computadoras de la Universidad, que se pueden encontrar en la política correspondiente (informatica.umce.cl/politicas). Consulte también la **política para la destrucción y eliminación de equipos y datos electrónicos.**

b. La eliminación o la reutilización de dispositivos personales que almacenaron datos de alto riesgo deben realizarse minuciosamente, eliminando todos los datos de alto riesgo. Consulte la **política para la destrucción y eliminación de equipos y datoselectrónicos**.

B. Seguridad de los datos

La forma en que maneja los datos no públicos depende de su clasificación de datos. Cuanto más restrictivos sean los datos, mejor se deberían proteger. Consulte la sección Medidas de seguridad

para el manejo de datos de la Política de seguridad de datos y sistemas para conocer los requisitos específicos; los siguientes son requisitos más generales.

1. **Protección de datos confidenciales en computadoras**

   a. Siga las especificaciones de seguridad informática establecidas anteriormente.

   b. Sepa qué datos están almacenados en su computadora, la confidencialidad de esos datos y qué políticas se aplican.

   c. Mantenga la retención de datos locales al mínimo. Confíe en el almacenamiento de la unidad, la escuela o la universidad.

   d. Siempre que sea posible, proteja con contraseña o cifre los datos confidenciales.

   e. Realice una copia de seguridad de los datos locales de forma regular y mantenga la copia de seguridad segura. Proteja las copias de seguridad con el mismo nivel de seguridad que los datos originales. Pruebe la recuperación de copias de seguridad periódicamente para verificar que funcione.

   f. Si usa una computadora compartida con otras personas, tome las precauciones adecuadas para proteger los datos confidenciales a los que otras personas pueden no estar autorizados a acceder. Siempre que sea posible, cree cuentas separadas para cada persona que use la computadora, estableciendo los permisos adecuados.

2. **Almacenamiento o transmisión de datos sensibles**

   a. No redistribuya datos confidenciales a otras personas dentro o fuera de la Universidad, a menos que usted sea una fuente y un distribuidor autorizado de esos datos y el destinatario esté autorizado para recibir esos datos.

   b. No permita que los datos confidenciales se almacenen en computadoras o servidores fuera de la universidad, a menos que dicho almacenamiento esté autorizado.

   c. Siempre que sea posible, los datos confidenciales deben transferirse en forma cifrada, por ejemplo, utilizando SSL (Secure Socket Layer) o SSH (Secure Shell).

   d. Recuerde que el correo electrónico no suele ser una forma segura de comunicación. Se debe tener cuidado para asegurarse de que el destinatario esté autorizado a recibir esos datos y que la dirección sea correcta.

   e. Los datos sensibles, incluida los números de la cedula de identidad o la información de la tarjeta de crédito, no deben enviarse sin cifrar por correo electrónico. Si es necesario utilizar el correo electrónico, utilice tecnología de cifrado para proteger la transmisión de datos confidenciales en el correo electrónico. Esto puede incluir el uso de VPN (redprivada virtual), SSL o el cifrado del mensaje en sí mediante software como PGP (Pretty Good Privacy).

   f. No transmita datos confidenciales utilizando tecnología de mensajería instantánea como Slack, WhatsApp y Facebook Messenger, que utilizan servidores fuera de la universidad. Estos servicios pueden permitir que personas no autorizadas accedan o almacenen datos confidenciales. Se recomienda que consulte con **el área de seguridad del Departamento de Informática** para obtener orientación.

   g. Tenga especial cuidado al enviar datos confidenciales por fax para asegurarse de que estén claramente marcados como confidenciales. Se debe hacer todo lo posible para garantizar que solo el destinatario previsto tenga acceso a la información enviada por fax.

h. Mantenga las máquinas de fax, impresoras y fotocopiadoras utilizadas para datos confidenciales en áreas seguras. Los faxes, las copias impresas y las copias de datos confidenciales deben recogerse con prontitud y manejarse de manera adecuada.

3. Eliminación de datos sensibles

a. Los datos confidenciales deben destruirse de manera que se evite la recreación.

b. Vuelva a formatear o destruya físicamente cualquier medio de almacenamiento extraíble (como discos duros externos, discos zip, cintas, CD, DVD o USB) que contengan datos confidenciales antes de deshacerse de ellos.

c. Triturar impresiones de datos sensibles.

d. Asegúrese de que los datos confidenciales se eliminen de los dispositivos que usa,incluidas las impresoras remotas, antes de desechar o volver a implementar esos dispositivos.

4. Responder a solicitudes de información

a. No comparta datos sensibles con representantes de la prensa (radio, televisión, medios impresos o electrónicos), otras personas o en foros públicos, como listas de correo o tablones de anuncios web, sin la debida autorización.

b. Remita las solicitudes para la divulgación de datos confidenciales al **área de seguridad del Departamento de Informática.**

Control de versiones

Autor	**Fecha**	**Versión**	**Motivo**
Trends	08/01/2020	V00	Creación
UMCE – Trends	19/05/2021	V01	Revisión
D. Informática – D. Jurídica	09/12/2021	V02	Aprobación

2º Se deja Constancia que la ejecución de esta Resolución Exenta no importa desembolso económico alguno para la Universidad**.**

Anótese, Comuníquese y Regístrese.

ELISA ADRIANA ARAYA CORTEZ

Firmado digitalmente por ELISA ADRIANA ARAYA CORTEZ
Fecha: 2022.03.01 16:44:33 -03'00'

ELISA ARAYA CORTEZ
RECTORA

Distribución:

- Archivo
- Dirección de administración y Finanzas
- Departamento de Informática

Dante Martinez Benavides

Firmado digitalmente por Dante Martinez Benavides
Fecha: 2022.02.28 16:52:30 -03'00'

UNIVERSIDAD METROPOLITANA
DE CIENCIAS DE LA EDUCACIÓN
SECRETARÍA GENERAL

Acuerdo 1042

SECRETARÍA GENERAL

JUNTA DIRECTIVA

Sesión ordinaria vía remota del 19 de enero del 2022

VISTOS **:** Las atribuciones de la Junta Directiva, establecidas en el Estatuto de la UMCE, DFL N° 1 de 1986, Artículo 13°, letra b.

CONSIDERANDO :

- La propuesta de la Jefa del Departamento de Informática.

ACUERDO N° 1042 **:** La Junta Directiva, reunida en sesión ordinaria vía remota del 19 de enero del 2022, aprueba, por unanimidad, las **Políticas Tecnológicas de la Información**, cuyos documentos descriptivos forman parte integrante del presente Acuerdo.

PABLO ANDRES CORVALAN REYES
Firmado digitalmente por PABLO ANDRES CORVALAN REYES
Fecha: 2022.01.20 22:52:31 -03'00'

PABLO CORVALÁN REYES
SECRETARIO GENERAL

Visión de TI en la UMCE

Convertirnos en el socio tecnológico de confianza de la UMCE, apoyando a la comunidad en el logro de sus objetivos, permitiendo la innovación y sirviendo a la misión de la universidad y la sociedad.

Misión de TI en la UMCE

Proveer a la comunidad de la UMCE con soluciones de TIC's simples, sin estrés, seguras, de fácil acceso, y trabajar de manera efectiva para brindar los más altos niveles de satisfacción de los usuarios.

UMCE

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

MEMORANDUM N°14 / 2022

A : SR. PABLO ANDRES CRISTIAN CORVALAN REYES .
SECRETARIO GENERAL

DE : SRA. BÁRBARA WALKER ALARCÓN
JEFA DEPARTAMENTO DE INFORMÁTICA

Asunto: ENTREGA DE POLÍTICAS APROBADAS

Fecha : 20-1-2022

Estimado Secretario General

Por medio del presente, Adjunto las políticas de Informáticas, Misión y Visión, aprobadas por la Honorable Junta Directiva el día 19 de Enero de 2022, para su publicación. Estas Políticas fueron presentadas en el marco del proyecto de Calidad UMC1857, con referencia al HITO "OE2. Fortalecer el área de informática para la gestión institucional a través de políticas, condiciones de operación e implementación de sistemas".

Sin otro particular, le saluda atentamente,

BARBARA AILEC WALKER ALARCON

BARBARA AILEC WALKER ALARCON
c=CL, st=REGIÓN METROPOLITANA DE SANTIAGO, l=SANTIAGO, o=UNIVERSIDAD METROPOLITANA DE CIENCIAS DE LA EDUCACION, ou=*, cn=BARBARA AILEC WALKER ALARCON, email=barbara.walker@umce.cl
2022.01.20 12:07:40 -03'00'

BÁRBARA WALKER ALARCÓN
JEFA DEPARTAMENTO DE INFORMÁTICA

UNIVERSIDAD METROPOLITANA
DE CIENCIAS DE LA EDUCACIÓN
SECRETARÍA GENERAL

MEMORANDUM N° 35

A : SR. JOSÉ RAFAEL CORTÉS V.
JEFE
DEPTO. JURÍDICO

DE : SECRETARIO GENERAL

FECHA: SANTIAGO, 20 de enero del 2022.

Me permito remitir a usted, para la emisión de la resolución correspondiente, el Acuerdo N° 1042 adoptado por la Junta Directiva en la sesión especial vía remota, del 19 de enero del 2022.

Sin otro particular, saluda atentamente a usted.

PABLO ANDRES CORVALAN REYES
Firmado digitalmente por PABLO ANDRES CORVALAN REYES
Fecha: 2022.01.20 23:03:25 -03'00'

PABLO CORVALÁN REYES
SECRETARIO GENERAL