UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, PROTECCIÓN DE DATOS Y NIVELES DE SOPORTE TÉCNICO DE LA UNIVERSIDAD ESTATAL DE MILAGRO

CONTENIDO

UNIVERSIDAD ESTATAL DE MILAGRO

CONSIDERANDO

Que, los numerales 1 y 2 del artículo 16 de la Constitución de la República del Ecuador, señala: "Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos; 2. El acceso universal a las tecnologías de información y comunicación";

Que, el numeral 19 del artículo 66 de la Constitución de la República reconoce y garantiza a las personas: "19. El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley";

Que, el artículo 350 de la Constitución de la República del Ecuador señala:" El sistema de educación superior tiene como finalidad la formación académica y profesional con visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo";

Que, el artículo 351 de la Constitución de la República del Ecuador establece: "El sistema de educación superior estará articulado al sistema nacional de educación y al Plan Nacional de Desarrollo; la ley establecerá los mecanismos de coordinación del sistema de educación superior con la Función Ejecutiva. Este sistema se regirá por los principios de autonomía responsable, cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad, autodeterminación para la producción del pensamiento y conocimiento, en el marco del diálogo de saberes, pensamiento universal y producción científica tecnológica global.";

Que, el artículo 355 de la Constitución de la República del Ecuador, señala: "El Estado reconocerá a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución.";

Que, el artículo 17 de la Ley Orgánica de Educación Superior, establece: "El Estado

reconoce a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los principios establecidos en la Constitución de la República.";

Que, la norma 410 sobre Tecnología de la Información, numeral 410-01, de las Normas de Control Interno de la Contraloría General del Estado, señala: "Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional. La Unidad de Tecnología de Información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además, debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo. (…)";

Que, la norma 410 sobre Tecnología de la Información, numeral 410-04, de las Normas de Control Interno de la Contraloría General del Estado, establece: "La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria. La Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran. Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales, además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información. (…)";

Que, la norma 410 sobre Tecnología de la Información, numeral 410-10 Seguridad de tecnología de información, de las Normas de Control Interno de la Contraloría

General del Estado, señala: “La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas: 1. Ubicación adecuada y control de acceso físico a la Unidad de Tecnología de Información y en especial a las áreas de: servidores, desarrollo y bibliotecas. 2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado. 3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación. 4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización. 5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados. 6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros; 7. Consideración y disposición de sitios de procesamiento alternativos. 8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.”;

Que, es necesario contar con un instrumento que regule la seguridad de la información, la protección de datos y los niveles de soporte técnico;

RESUELVE:

Expedir las siguientes:

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, PROTECCIÓN DE DATOS Y NIVELES DE SOPORTE TÉCNICO DE LA UNIVERSIDAD ESTATAL DE MILAGRO

TÍTULO I
PRINCIPIOS GENERALES

CAPÍTULO I
DEL OBJETO, ÁMBITO Y ALCANCE

Política 1.- Objeto. - Las presentes políticas tienen por objeto proporcionar un marco de seguridad que garantice la protección de la información de la Universidad Estatal de Milagro frente a la pérdida, daño o el acceso no autorizado, al tiempo que apoya las necesidades de intercambio de información de nuestra cultura organizacional.

Establece al acceso a la información como un componente indispensable en el aseguramiento de la calidad para lograr la conducción y consecución de los objetivos institucionales, definidos en la misión, por lo cual se asegura que la información está protegida de manera adecuada independientemente de la forma que sea manejada, procesada, transportada o almacenada.

Política 2.- Ámbito. - Las presentes políticas serán aplicadas de manera obligatoria por las autoridades, personal académico y administrativo, trabajadores, estudiantes y demás personal o terceros que intervengan en la ejecución de los procesos de la Universidad Estatal de Milagro.

Política 3.- Definiciones. - Las definiciones utilizadas en estas políticas son las siguientes:

a) **Activo:** cualquier componente (tecnológico, electrónico, software, hardware, o de infraestructura) que forme parte dentro de los bienes de la institución.
b) **Autenticación:** es el procedimiento de comprobación que permite verificar si un usuario de un sitio web o un servicio es quien dice ser.
c) **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
d) **Cifrado:** es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrado) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
e) **Control:** es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
f) **Derechos de autor:** es un conjunto de normas y principios que regulan los

derechos morales y patrimoniales que la ley conoce a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

g) **Disponibilidad:** es la garantía que los usuarios autorizados tienen acceso a la información y a los archivos asociados cuando lo requieren.
h) **Equipo de cómputo:** dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
i) **Inventario de activos tecnológicos:** es una lista ordenada y documentada de los activos perteneciente a la institución.
j) **Custodio del activo tecnológico:** es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los archivos de información confiados.
k) **TICS:** Dirección de Tecnología de la Información y Comunicaciones.

TÍTULO II
SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO I
NIVELES DE CLASIFICACIÓN DE LA INFORMACIÓN

Política 4.- Clasificación de la información. - Toda la información de la Universidad Estatal de Milagro se clasifica en niveles según su sensibilidad y los riesgos asociados con la divulgación. El nivel de clasificación determina las protecciones de seguridad que deben utilizarse para la información.

Los niveles de clasificación son:

a) **Confidencial**: acceso restringido que requiere autorización del titular para su acceso.
b) **Restringido**: directores de área y empleados clave tienen acceso.
c) **Público**: todas las personas, dentro y fuera de la organización, tienen acceso.

En función a la clasificación, la información universitaria debe estar adecuadamente protegida contra el acceso no autorizado, la pérdida y el daño.

SECCIÓN I
DE LA INFORMACIÓN DE ACCESO CONFIDENCIAL

Política 5.- Información de acceso confidencial. - Es aquella Información o documentación, en cualquier formato, final o preparatoria, haya sido o no generada por el sujeto obligado, derivada de los derechos personalísimos y fundamentales, y requiere expresa autorización de su titular para su divulgación, que contiene datos que al revelarse, pudiesen dañar los siguientes intereses privados:

El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.
La información considerada confidencial será:

a. Datos personales cuya difusión requiera el consentimiento de sus titulares y deberán ser tratados según lo dispuesto en la Ley Orgánica de Protección de Datos Personales;
b. Las patentes
c. Derechos de autor
d. Códigos de programación

SECCIÓN II
DE LA INFORMACIÓN DE ACCESO RESTRINGIDO

Política 6.- Información de acceso restringido. - Es aquella a la que sólo ciertos miembros de la institución tienen acceso.
La información considerada restringida será:

a. Información médica
b. Documentos internos relacionados con los estudiantes

SECCIÓN III
DE LA INFORMACIÓN DE ACCESO PÚBLICO

Política 7.- Información de acceso público. - Todo tipo de dato en documentos de cualquier formato, final o preparatoria, haya sido o no generada por el sujeto obligado, que se encuentre en poder de los sujetos obligados por la Ley Orgánica de Transparencia y Acceso a la Información Pública, contenidos, creados u obtenidos por ellos, que se encuentren bajo su responsabilidad y custodio o que se hayan producido con recursos del Estado.

La información considerada de acceso público, será:

a. Resoluciones del Órgano Colegiado Superior.
b. Presupuesto anual que maneja la institución
c. Información financiera y contable
d. Información sobre la ejecución presupuestaria
e. Informes de rendición de cuentas
f. Normativas internas
g. Actas de sesiones del Directorio
h. Informe anual sobre el cumplimiento del derecho de acceso a la información pública.
i. Distributivo de remuneraciones de administrativos, docentes y trabajadores.

CAPÍTULO II
DEL CONTROL DE ACCESO

Política 8.- Control de claves y nombres de usuario a los sistemas de información institucionales (SGA, SAGEST). - Están restringidos según los perfiles de usuario definidos. Los permisos para personal administrativo, son asignados mediante formulario firmado electrónicamente, donde se confirma la asignación de los permisos a los sistemas de información, donde el usuario se hace responsable de su perfil asignado. Se forzará el cambio de clave para todos los usuarios cada 30 días.

Política 9.- Control de las contraseñas y uso de equipos de red. - Será responsabilidad de Recursos Tecnológicos y dichas contraseñas son codificadas y almacenadas de forma segura.

Política 10.- Claves de administrador de los sistemas. - Serán conservadas por la Dirección de Tecnología de la Información y Comunicaciones (TICS) y el Área de Desarrollo y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

Política 11.- Claves de administrador de los servidores. - Serán conservadas por la Dirección de Tecnología de la Información y Comunicaciones (TICS), Área de Desarrollo y el Área de Servicios Informáticos, son cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

Política 12.- Responsabilidad de uso de la cuenta. - El propietario de una cuenta es el único responsable de su uso, cuando se detecte una actividad prohibida, la UNEMI responsabilizará al propietario de la misma.

Política 13.- Elaboración, mantenimiento y actualización de procedimientos. - Las áreas de recurso tecnológico, desarrollo y sistemas informáticos elabora, mantiene y actualiza los procedimientos y guías para la correcta definición, uso y complejidad de claves de usuario.

Política 14.- Cancelación de cuentas de los usuarios. - La Dirección de Tecnología de la Información y Comunicaciones (TICS), es la encargada de expedir un certificado de cancelación de las cuentas de usuario asignadas para el uso de recursos de tecnologías de la información de la institución, quedando prohibido cualquier uso comercial y/o privado no autorizado de los recursos informáticos de la UNEMI.

Política 15.- Identificación, clasificación y valoración de activos tecnológicos. - La Dirección de Tecnología de la Información y Comunicaciones (TICS) en coordinación con la Gestión de Activos Fijos tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la institución.

Política 16.- Seguridad física y entorno de los equipos del cuarto de datos. - Para la seguridad de los equipos se seguirá lo siguiente:

a) Se debe tener acceso controlado y restringido a los cuartos de servidores principales y a los cuartos de comunicaciones de diferentes bloques dentro de la institución y serán de uso exclusivo de TICS.
b) Los servidores que contengan información y servicios institucional deben ser mantenidos en un ambiente seguro y protegido por los menos con:

1. Controles de acceso y seguridad física.
2. Detección de incendios.
3. Controles de humedad y temperatura.
4. Bajo riesgo de inundación.
5. Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Política 17.- Del acceso remoto. - El acceso remoto a servicios de red ofrecidos por la UNEMI debe estar sujeto a medidas de control definidas por el TICS, las cuales deben incluir acuerdos escritos de seguridad de la información, estas son VPN-PPT-PPP.

Política 18.- De las prohibiciones. - La acciones que dañen, retarden, pongan en peligro o el acceso no autorizado al trabajo de otros usuarios, están prohibidas, son éticamente reprobables y se aplicará las normas internas, sin perjuicio de las civiles o legales que resulten pertinentes.

Política 19.- Acceso a los recursos informáticos y telemáticos. - En ningún caso se podrá acceder a los recursos informáticos y telemáticos con las finalidades siguientes:

a) Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.
b) Difundir contenidos contrarios a los principios enunciados en los Estatutos de la UNEMI.
c) Dañar los sistemas físicos y lógicos de la UNEMI, de sus proveedores o de terceras personas.
d) Introducir o difundir en la red virus informáticos o cualesquiera otros sistemas físicos o lógicos que sean susceptibles de provocar los daños anteriormente citados.
e) Usar cuentas de usuario sin autorización. Obtener la contraseña de acceso de una cuenta de usuario sin la autorización del propietario. Comunicar a otros la contraseña para que puedan entrar en la cuenta.
f) f) Usar la red u ordenadores de la UNEMI para conseguir acceso no autorizado a cualquier ordenador.
g) Realizar con conocimiento de causa cualquier acto que interfiera en el correcto funcionamiento de los ordenadores, terminales, periféricos, red de comunicaciones, etc.
h) Instalar o ejecutar en cualquier punto de la red informática programas o ficheros que deterioren o incrementen en exceso la carga en cualquier punto de la misma, hasta el límite de llegar a perjudicar a otros usuarios o al rendimiento de la propia red. Esto incluye cualquier tipo de ensayo, experimento o actividad

que incluso pudiendo ser considerada legítima perjudique el buen funcionamiento de la red.

i) Instalar o ejecutar en cualquier punto de la red informática programas o ficheros que traten de descubrir información distinta de la del propio usuario, en cualquier elemento de la red. Esto incluye los sniffer, scanner de puerto, etc.
j) Intentar sobrepasar protecciones de datos o sistemas de seguridad informática.
k) Violar la privacidad de los datos y el trabajo de los otros usuarios.

Algunas de las actividades anteriormente citadas no serán consideradas como uso incorrecto cuando estén autorizadas por la UNEMI y sean realizadas por el TICS para incrementar la seguridad informática.

Política 20.- De la conexión a la red de comunicaciones. - La conexión a la red de comunicaciones de un nuevo equipo informático es autorizado por el TICS quien proporcionará a dicho equipo una dirección IP. Queda prohibido el uso de IPs no proporcionadas por el TICS o el intercambio de ellas.

Política 21.- De las direcciones IP. - La UNEMI, a través de la Dirección de Tecnologías de la Información y Comunicación (TICS), gestionará los rangos de direcciones IP que le han sido asignados por RedUnemi en base a criterios técnicos, de ahorro y eficiencia.

CAPÍTULO II
DE LA UBICACIÓN DE LOS EQUIPOS Y LOS PROBLEMAS TÉCNICOS

Política 22.- Ubicación de los equipos. - Los equipos se alojarán en los servidores de “Google Cloud”, con ello el primer nivel de soporte está ligado a la institución.

a) Al detectarse y/o conocer de una incidencia (falta de conectividad a los diferentes servicios y sistemas), se realiza el monitoreo y detección de posibles causas
b) Se descarta cada una de las causas que pueden estar ocasionando la falta de servicios
c) Si se detecta el origen del incidente en los predios, se brinda el soporte al usuario informando las acciones que se están ejecutando para solventar el incidente.

Política 23.- De los problemas técnicos. - Cuando se originen problemas en cualquiera de los niveles antes mencionados, los usuarios de la comunidad universitaria solicitarán apoyo técnico de la siguiente forma:

1. Se recepta mediante correo electrónico servicios.informaticos@unemi.edu.ec.
2. Se da un tiempo de respuesta de la siguiente forma:
   -En horario de 8:00 – 22:00 en 2 horas aproximadamente.
   -En horario de 22:01 – 7:59 en 10 horas aproximadamente.

TÍTULO III
NIVELES DE SOPORTE

CAPÍTULO I
NIVELES DE SOPORTE EN GESTIÓN DE INCIDENTES

Política 24.- De los niveles de soporte. - Los niveles de soporte son:

a) **Nivel 1.-** Aquí se presentan y resuelven la incidencia en problemas tales como: líneas físicas de comunicación, resolución de usuarios y contraseñas, instalación / reinstalación de softwares básicos, verificar la configuración correcta de hardware y software y asistencia mediante navegación de menús de aplicación. El objetivo de este primero nivel e resolver aproximadamente el 80% de problemas habituales antes de escalar a otro nivel.

b) **Nivel 2.-** Es el grupo basado en help desk, pues los técnicos tienen conocimientos más especializados en el área tecnológica, los problemas que se pueden presentes son en bases de datos, redes de comunicación, sistemas operativos, sistemas de información, entre otras.

c) **Nivel 3.-** Son el soporte back-end este grupo se encarga del desarrollo de soluciones a los problemas además tiene las mismas responsabilidades que los técnicos de nivel 2 y adicional verificará:
   1. Si la solución de problema es factible o no.
   2. Si se requiere información adicional para la resolución.

3. Tener el tiempo suficiente.
4. Identificar la mejor solución.

DISPOSICIONES GENERALES

PRIMERA. - Las presentes políticas serán difundidas y comunicadas a toda la comunidad universitaria a través de su página web; y, estará a disposición de todas las partes interesadas.

SEGUNDA. - El presente instrumento será revisado cada año o cuando haya cambios operacionales, con el fin de que sea actualizado por la Dirección de Tecnologías de la Información y la Comunicación.

TERCERA. - Las medidas a considerar por la violación a las presentes políticas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo a las normativas vigentes según el caso.

Entre otras medidas a aplicar, se contemplan las siguientes: desconectar / deshabilitar las cuentas en los servidores, e inhabilitar el acceso a la red del ordenador o grupo de ordenadores que están generando el mal funcionamiento.

CUARTA. - La Dirección de Servicios Informáticos será la responsable del aseguramiento de los recursos adecuados para implementar y mantener las presentes políticas, verificar el cumplimiento y fomentar una cultura de seguridad.

DISPOSICION FINAL

ÚNICA. - Quedan derogadas o reformadas todas las disposiciones que se opongan a la presente norma que entrará en vigencia a partir de su ratificación por OCS.

CERTIFICACIÓN

La infrascrita Secretaria General de la Universidad Estatal de Milagro, CERTIFICA que, las POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, PROTECCIÓN DE DATOS Y NIVELES DE SOPORTE TÉCNICO DE LA UNIVERSIDAD ESTATAL DE MILAGRO, fue aprobada por la primera autoridad ejecutiva, mediante RESOLUCIÓN DE DESPACHO-UNEMI-R-2023-Nro. 54, el 07 de diciembre de 2023.

Milagro, 07 de diciembre de 2023.

Abg. Stefania Velasco Neira, Mgtr.
SECRETARIA GENERAL

UNIVERSIDAD ESTATAL DE MILAGRO
UNEMI
SECRETARIA GENERAL