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

Versión: 1.0 Código: POL.05

UNIVERSIDAD ESTATAL DE MILAGRO
UNEMI
Evolución Académica

www.unemi.edu.ec

Ciudadela Universitaria Km. 1 ½ vía Km 26
Teléfonos: (04) 2715081 (04) 2715079
Milagro – Guayas – Ecuador

Contenido

UNIVERSIDAD ESTATAL DE MILAGRO

CONSIDERANDO

Que, el Art. 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 art. 351 de la Constitución de la República del Ecuador establece que, *"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, la Constitución de la República en el art. 355, reconoce 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, la Ley Orgánica de Educación Superior, publicada en el Registro Oficial No.298, del 12 de octubre del 2010, en el art. 17 señala: *"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, las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que dispongan de recursos públicos, en el numeral 410, *TECNOLOGÍA DE LA INFORMACIÓN*, 410-01 Organización informática: determina que, *"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, las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que dispongan de recursos públicos, en el numeral 410-04 Políticas y procedimientos, determina que, *"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, las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que dispongan de recursos públicos, en el numeral 410-10 Seguridad de tecnología de información, determina que, *"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, el Reglamento del Órgano Colegiado Académico Superior de la Universidad Estatal de Milagro, en el Art. 43, determina que, *"(…) Los instructivos, manuales de procesos y procedimientos, además de políticas institucionales serán aprobadas por la o el Rector, en calidad de Presidente del Comité de Gestión de Calidad de Servicio y el Desarrollo Institucional";*

Que, el Rector en ejercicio de sus facultades y atribuciones constitucionales y legales,

RESUELVE:

Expedir las siguientes:

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y NIVELES DE SOPORTE DE LA UNIVERSIDAD ESTATAL DE MILAGRO.

TÍTULO I
PRINCIPIOS GENERALES

CAPITULO I
OBJETO Y ALCANCE

Política 1.- El objeto de las presentes políticas es la de establecer 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.- Las políticas incluidas en este documento constituyen una parte fundamental de la seguridad informática de UNEMI y se convierten en la base para la implantación de controles, procedimientos y estándares que deben ser definidos, para las amenazas que enfrentan amenazas de seguridad que incluyen entre muchas otras: el fraude por computadora, el sabotaje, el vandalismo, el fuego, los robos, las inundaciones e ingreso sin autorización, las posibilidades de daño y la pérdida de la información por causa de código malicioso, el mal uso o ataques de denegación de servicios se hacen cada vez más comunes.

Política 3.- El alcance de las presentes políticas de seguridad de la información tratarán de cubrir parte de los aspectos administrativos y académicos de control que deben ser cumplidos por los directivos, administrativos, docentes, estudiantes y terceros que laboren o tengan relación con la UNEMI, para conseguir un adecuado nivel de protección y calidad de la información.

CAPITULO II
DEFINICIONES

Política 4.- 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 Tecnología de la Información y las Comunicaciones.

TÍTULO II
SEGURIDAD DE LA INFORMACIÓN

CAPITULO I
CONTROL DE ACCESO

Política 5.- El 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 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 6.- El control de las contraseñas y uso de equipos de red es responsabilidad de Recursos Tecnológicos.- Dichas contraseñas son codificadas y almacenadas de forma segura.

Política 7.- Las claves de administrador de los sistemas, son conservadas por la Dirección del Departamento de Tecnologías de la Información y Comunicación (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 8.- Las claves de administrador de los servidores, son conservadas por la Dirección de Tecnologías de la Información y Comunicación (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 9.- 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 10.- Las áreas de recurso tecnológico, desarrollo y sistemas informáticos elabora, mantienen y actualiza los procedimientos y guías para la correcta definición, uso y complejidad de claves de usuario.

Política 11.- El requisito para la terminación de relación contractual -o laboral del personal de la Universidad.- el TICS es la 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 12.- Identificación, clasificación y valoración de activos tecnológicos.- El TICS en coordinación con Activos Fijos tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la institución.

Política 13.- Seguridad física y del entorno de los equipos del cuarto de datos

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:
   - Controles de acceso y seguridad física.
   - Detección de incendios.
   - Controles de humedad y temperatura.
   - Bajo riesgo de inundación.
   - Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Política 14.- 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 15.- Las acciones. Que intencionadamente rompan, retarden, pongan en peligro o accedan al trabajo de otros usuarios, sin autorización específica, están prohibidas, son éticamente reprobables y se aplicará las normas internas, y judicialmente si fuera preciso.

Política 16.- 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) 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 17.- 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 18.- Direcciones IP. La UNEMI, a través del TICS, gestionará los rangos de direcciones IP que le han sido asignados por RedUnemi en base a criterios técnicos, de ahorro y eficiencia.

CAPITULO II
NIVELES DE SOPORTE

Política 19.- Los equipos se están alojados en el Data Center de CEDIA, con ello el primer nivel de soporte está ligado a la institución. *Ver Anexo No. 1.*

- 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
- Se descarta cada una de las causas que pueden estar ocasionando la falta de servicios
- 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 20.- Cuando se originan problemas en cualquiera de los niveles antes mencionados a los usuarios de la comunidad universitaria se resuelve de la siguiente forma:

- Se recepta mediante correo electrónico tics@unemi.edu.ec y/o tic@unemi.edu.ec, o llamas telefónicas a 042715081 – 0422715079 a las extensiones 3306 – 3305 – 3310 – 3312 – 3315.
- 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 8 horas aproximadamente.

CAPITULO III
NIVELES DE SOPORTE EN GESTIÓN DE INCIDENTES

Política 21.- 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:

- Si la solución de problema es factible o no.
- Si se requiere información adicional para la resolución.
- Tener el tiempo suficiente.
- Identificar la mejor solución.

d) **Nivel 4.-** Es el proveedor de los servicios de internet, servidores entre otros servicios que ofrece CEDIA. De originarse el incidente por parte del proveedor, se escalan a los niveles de servicio que se detallan:

Política 22.- **Por parte del proveedor del servicio:** CEDIA cumple con los Niveles de Servicio detallados en la siguiente tabla.

Servicio de Red Avanzada e Internet:

Denominación: Disponibilidad de servicio

Política 23.- Niveles de Servicio. Se entiende como **"disponibilidad"** al tiempo medido en horas, que cada enlace está en servicio, con los parámetros anotados en este numeral.
La disponibilidad será medida mensualmente para cada uno de los enlaces de internet, red avanzada y/o transmisión de datos que haya contratado el MIEMBRO para sus diferentes sedes, considerando las capacidades de cada uno de ellos (incluyendo el enlace de backup en caso de tenerlo). Según el resultado de esta medición, se definirá el Valor Mensual a Pagar, conforme a lo expresado en el numeral 5.4 de esta tabla.

a) La disponibilidad (D) mínima mensual contratada para cada enlace es:

Servicio	Indicador	Observaciones
Internet/Red Avanzada/Datos	99,6%	Con una única última milla
	99,8%	Con doble última milla

Para porcentajes de disponibilidad menores a los arriba indicados por cada enlace, se aplicará el cálculo del descuento mensual descrito en el numeral 5.4.

El valor de disponibilidad se calculará con la siguiente expresión:

$$D = \left(1 - \frac{TI - TM}{TT}\right) * 100$$

Dónde:

D (%) = Disponibilidad mensual del enlace, expresado como un porcentaje.

TI (horas)=Tiempo Indisponible, tiempo que el servicio estuvo indisponible o fuera de servicio en horas durante el mes. Este tiempo inicia desde la asignación de un ticket por parte de CEDIA o el proveedor, en respuesta del reporte realizado por el miembro.

Las fallas masivas se registrarán como un solo ticket, tomando como un tiempo único de indisponibilidad de todos los enlaces comprometidos en esa falla.

TT (horas)=Tiempo Total, tiempo total de horas en un mes. Este valor es fijo, y dependiendo del mes, será igual a:

- 672 horas (28 días).
- 696 horas (29 días).
- 720 horas (30 días).

- 744 horas (31 días).

TM (horas)=Tiempo de Mantenimiento, tiempo que el enlace estuvo fuera de servicio debido a mantenimientos preventivos planificados por CEDIA y previamente comunicados al MIEMBRO; o a cualquiera de los motivos considerados como caso fortuito o fuerza mayor siempre que tales eventos, según lo establecido en el artículo 30 del Código Civil Ecuatoriano, impidan que de forma continua las partes cumplan con sus obligaciones contractuales, sin derecho a reclamo de indemnización alguna entre las partes, ni retribución de ninguna clase, sin perjuicio de que, también se contemplen dentro de este tiempo los eventos que se indican a continuación:

b) Desastres naturales, atentados, hurto, vandalismo, accidente, incendio, alteración del orden público, etc., que afecten las instalaciones, equipos y/o facilidades de CEDIA.

c) Tiempo de movilización (tm) al sitio de falla (en caso de requerirse), cuyos valores máximos se ajustarán a la siguiente tabla:

Tipo	DESCRIPCIÓN	Tm (horas)
Tipo 0	Quito y Guayaquil	1
Tipo 1	Capitales de provincia – Sierra y Costa	4
Tipo 2	Capitales de provincia – Oriente	8
Tipo 3	Fuera de capitales provinciales.	12
Tipo 4	Región Insular.	24

d) A los tiempos de movilización indicados en la tabla anterior, se debe sumar una (1) hora del tiempo de preparación que requiere CEDIA para asistir al lugar del incidente.

- Fallas en las instalaciones del MIEMBRO tales como acometidas internas, ducterías internas, sistemas de tierra, reguladores, baterías, plantas eléctricas y UPS´s, aplicaciones y protocolos utilizados por el MIEMBRO, equipos de cómputo y equipos de comunicación de datos para LAN, falta de permisos apropiados para el acceso de CEDIA a las instalaciones del MIEMBRO.
- Tiempo que tome al miembro en realizar todas las actividades necesarias para la conmutación de tráfico por la ruta redundante habilitada.
- Tiempo que se genere en otorgar los permisos apropiados para el acceso a las instalaciones del MIEMBRO.
- Interrupciones autorizadas y/o requeridas por el MIEMBRO.
- Tiempos debido a la falta de entrega de información por parte del MIEMBRO que no permita realizar una evaluación eficaz de la falla reportada.
- Prorroga de trabajos por cumplimiento de normativas de SISO.

- Problemas en donde se detecte que la falla fue originada en el equipamiento del miembro o por mala manipulación de los equipos de CEDIA, sin el consentimiento de su personal técnico.
- Problemas que sean originados por fallas en extremos del enlace provistos por otro operador diferente de CEDIA, a menos de que se trate de: a) un contrato en donde CEDIA asume la administración y facturación por circuito completo; o, b) la subcontratación de terceros por parte de CEDIA

Denominación: Disponibilidad de servicio
Niveles de Servicio: Calidad del Enlace
La Calidad de un Enlace contempla anchos de banda (BW), retardos y errores.

e) **Ancho de Banda**

- Este valor será definido por el MIEMBRO y garantizado por CEDIA de acuerdo a los paquetes ofertados y contratados.

Retardos

- El retardo se mide, como referencia, utilizando ICMP a través del comando "ping" (echo request / echo reply).
- Según el tipo de enlace, los tiempos promedios de delay, considerando un canal sin carga, un tamaño de paquete de 100 bytes, y 1000 ping de prueba, deberán ser los siguientes:
- Locales < 30ms – pérdidas menores al 2%
- Interurbanos < 90ms – pérdidas menores al 2%
- Internacionales < 100ms – pérdidas menores al 3%

Errores

- Los enlaces de Red Avanzada, datos o Internet, en donde sea factible la medición, se debe garantizar una tasa de error de bit inferior a $1x10^{-8}$ (BER).

Denominación: Horario de Soporte Técnico.

Política 24.- Niveles de Servicio: CEDIA cuenta con un Centro de Servicio Técnico, aquí trabaja personal con la experiencia y el conocimiento necesario, de tal manera que brindan el soporte apropiado al MIEMBRO para superar cualquier inconveniente o problema en los enlaces. Este horario es de: **7x24x365**.

Servicio de virtualización

a) Soporte 8x5 (lunes a viernes en horarios 8:00 a 13:00 – 15:00 a 18:00). El servicio de soporte es exclusivamente para el Servidor Virtual Aprovisionado a nivel de infraestructura de Cómputo y almacenamiento provisto por CEDIA, la migración,

operación y mantenimiento del Sistema Operativo y/o aplicaciones que serán instaladas en el Servidor Virtual es de completa responsabilidad de la Institución contratante.

b) Se ofrecerá soporte durante la migración en la modalidad 8x5 (lunes a viernes en horarios 8:00 a 13:00 – 15:00 a 18:00).
c) Respaldo completo de la VM a través de Veeam (1 x semana hasta 8 versiones)
d) Administración de Seguridades perimetrales de infraestructura.
e) Monitoreo de tráfico y capacidades aprovisionadas.
f) Red Ipv6 /64, 1 dirección IPv4 Pública x servidor virtual
g) Disponibilidad: 99,6%

Política 25.- Seguridad_CEDIA. - Se compromete a tratar su Información Personal con privacidad, confidencialidad y seguridad y a proteger sus datos personales mediante todos los medios técnicos a su alcance de la pérdida, mal uso, acceso no autorizado, alteración y destrucción.

Empresas externas a CEDIA que tengan acceso a sus datos personales en relación con los servicios prestados a CEDIA estarán obligados a mantener la información confidencial y no tendrán permiso para utilizar esta información para cualquier otra finalidad que no sea desempeñar los servicios que están realizando para CEDIA. Al proporcionarnos su información, usted acepta que las referidas empresas externas a CEDIA puedan tener acceso a sus datos personales en razón de los servicios que estas empresas prestan a CEDIA. En algunos casos, será necesario que transfiramos sus consultas a compañías afiliadas a CEDIA. También en estos casos sus datos serán tratados de manera confidencial. CEDIA podría llegar a revelar datos personales si fuese debidamente requerido por ley, tribunal o autoridad competente.

Política 26.- Compromiso de la Dirección. -

- Crear una comisión técnica denominada “COMITÉ DE SEGURIDAD DE LA INFORMACIÓN”.
- Fomentar una cultura de seguridad.
- Socializar las Políticas a todos los funcionarios de la institución.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- Verificar por el cumplimiento de las políticas aquí mencionadas.

Política 27.- Acciones técnicas al no ser contempladas las presentes políticas. - Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los docentes, estudiantes, administrativos, trabajadores, personal externo y proveedores de la UNEMI. Por tal razón, las no observancias a las Políticas de Seguridad de la

Información deberán clasificarse a objeto de poder aplicar medidas preventivas y correctivas con el fin mitigar posibles afectaciones contra la seguridad de la información.

La UNEMI podrá suspender el uso de estos recursos a aquellos usuarios que contravengan la presente normativa y en los casos en los que cualquier circunstancia sobrevenida lo amerite.

Si la posible afectación causada a otros usuarios o al servicio, por un usuario, se entiende que no afecta de forma inmediata al buen funcionamiento del servicio, se le notificará su mal proceder mediante correo electrónico u ordinario. Si, por el contrario, se entendiera que el trastorno producido altera el buen funcionamiento del servicio, el TICS tendrá la facultad de tomar las medidas necesarias para restaurar de forma inmediata el correcto servicio.

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.

DISPOSICIONES

PRIMERA.- Las presentes políticas será difundida y comunicada a toda la comunidad universitaria, en forma personificada, 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.

CERTIFICACIÓN

La infrascrita Secretaria General(E) de la Universidad Estatal de Milagro, CERTIFICA: Que las **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y NIVELES DE SOPORTE TÉCNICO DE LA UNIVERSIDAD ESTATAL DE MILAGRO**, fueron aprobadas, por la primera autoridad ejecutiva de la UNEMI, mediante Resolución de Despacho N° 2018-005, el 21 de diciembre de 2018.

Milagro, 21 de diciembre de 2018

Lic. Diana Pincay Cantillo
SECRETARIA GENERAL(E)

UNIVERSIDAD ESTATAL DE MILAGRO
UNEMI
SECRETARIA GENERAL

A N E X O S

Anexo N.1 DIAGRAMA DE ATENCIÓN A USUARIOS (MESAS DE AYUDA/SERVICIOS)