UNEMI

UNIVERSIDAD ESTATAL DE MILAGRO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

INTRODUCCIÓN 3

ASPECTOS GENERALES 3

1. OBJETIVO 3
2. ÁMBITO DE APLICACIÓN 3
3. DEFINICIONES 4

DEL USO DE LA INFORMACIÓN Y LOS ACTIVOS DE INFORMACIÓN INSTITUCIONAL 7

1. PROPIEDAD Y USO 7
2. DISPOSITIVOS, EQUIPOS TECNOLÓGICOS Y ELECTRÓNICOS 8
3. RESPALDOS DE INFORMACIÓN 9
4. DESTRUCCIÓN DE INFORMACIÓN 9
5. CLASIFICACIÓN DE LA INFORMACIÓN 9
6. ACUERDOS DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN 10
7. USO DE ANTIVIRUS 11
8. CONTROL DE ACCESO A APLICACIONES INSTITUCIONALES, SISTEMA OPERATIVO Y SISTEMAS DE GESTIÓN GUBERNAMENTAL 11
9. USO DEL INTERNET 12
10. USO DEL CORREO ELECTRÓNICO INSTITUCIONAL 12
11. REDES SOCIALES OFICIALES 13
12. INSTALACIÓN DE SOFTWARE 14
13. CREDENCIALES DE ACCESO A LOS ACTIVOS DE INFORMACIÓN INSTITUCIONAL 14
14. SEGURIDADES DE REDES LAN E INALÁMBRICAS 15
15. SEGURIDADES DE REDES PRIVADAS VIRTUALES (VPN) 15
16. ACCESO REMOTO 15
17. REDES INALÁMBRICAS NO AUTORIZADAS 16
18. USO DE LA INTELIGENCIA ARTIFICIAL 16
19. AUDITORÍA Y EVALUACIÓN DE VULNERABILIDADES 17
20. MONITOREO DE LA SEGURIDAD DE LA INFORMACIÓN 17
21. ACTUACIÓN FRENTE A INCIDENTES DE CIBERSEGURIDAD 18
22. MEDIDAS CORRECTIVAS O DISCIPLINARIAS 18

DISPOSICIONES GENERALES 19

DOCUMENTOS DE REFERENCIA 20

FIRMAS DE RESPONSABILIDAD 21

INTRODUCCIÓN

La creación de esta Política de Seguridad de la Información (PSI) responde a la necesidad de establecer un marco claro y efectivo que precautele la confidencialidad, integridad y disponibilidad de los datos manejados. Las PSI permiten implementar un conjunto de medidas para salvaguardar tanto la información física como digital, basadas en estos tres principios fundamentales.

La importancia de contar con esta política radica en su capacidad para proteger los activos informáticos frente a amenazas internas y externas, así como para asegurar el cumplimiento de normativas y regulaciones vigentes. La tecnología de la información enfrenta amenazas cada vez mayores, lo que requiere esfuerzos continuos para adaptarse y gestionar los riesgos que se presentan. Esto incluye establecer requisitos para la protección de la información, así como herramientas de comunicación y servicios tecnológicos que apoyen los procesos administrativos y académicos de la Universidad Estatal de Milagro (UNEMI).

Esta política es desarrollada y supervisada por el Oficial de Seguridad de la Información (OSI), quien es responsable de su implementación efectiva y su alineación con los objetivos estratégicos de la organización cuyo propósito es definir los objetivos, dirección, principios y reglas básicas que guiarán la gestión de la seguridad de la información dentro de nuestra organización.

ASPECTOS GENERALES

1. OBJETIVO

Disponer de una política de seguridad y uso eficiente de las tecnologías de la información y comunicación (TIC), que permitan proteger y asegurar la disponibilidad, integridad y confidencialidad de los activos de información, en apoyo a los objetivos estratégicos de la Universidad Estatal de Milagro.

2. ÁMBITO DE APLICACIÓN

La presente política será de cumplimiento obligatorio para todos los miembros de la comunidad universitaria, incluidos los usuarios externos que intervengan en la ejecución de los procesos de la Universidad Estatal de Milagro.

3. DEFINICIONES

Para la aplicación de la presente política, se considerarán las siguientes definiciones:

1. **Activos de Información Crítica:** Recursos que contienen información indispensable para la operación de la Universidad Estatal de Milagro (como, por ejemplo: información de configuraciones sobre las plataformas institucionales, software de bases de datos, código fuente y aplicaciones sensibles de los activos);

2. **Activos de información Institucional:** Es todo lo que procesa, genera o almacena información relacionada a los distintos procesos de la Universidad Estatal de Milagro, como pueden ser hardware, software, nube, documentos físicos, documentos electrónicos, personas, entre otros;

3. **Aplicaciones Institucionales:** Software desarrollado o adquirido por la Universidad Estatal de Milagro con el fin de prestar un servicio y apoyar las actividades esenciales y de soporte de la Universidad Estatal de Milagro;

4. **Cifrado:** Transformación criptográfica de datos (denominada "texto sin formato") en una forma diferente (llamada "texto cifrado") que oculta el significado original de los datos y evita que la forma original de estos sea utilizada. El proceso inverso correspondiente es el “descifrado", que representa una transformación que restaura los datos cifrados a su forma original;

5. **Comunidad Universitaria:** Son todas las autoridades, personal académico, investigadores, personal administrativo, trabajadores y estudiantes de la Universidad Estatal de Milagro;

6. **Confidencialidad:** Implica que la información no está disponible, no es de libre acceso y que no debe ser divulgada a personas, entidades públicas y privadas o procesos no autorizados;

7. **Credenciales institucionales:** Es el usuario y contraseña creadas para el uso de las aplicaciones institucionales, como: sistemas de gestión, sistemas académicos o el correo institucional, que posibilita realizar o ejecutar un determinado proceso, función o actividad, asignadas a un usuario o área;

8. **Datos personales:** Información de carácter personal o íntimo, que es materia de protección, en virtud de los establecido en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos; y Ley Orgánica de Protección de Datos Personales;

9. **Disponibilidad:** Información institucional que deberá estar disponible y utilizable en el momento que sea requerida por una persona o entidad autorizada;

10. **Dispositivo tecnológico:** Cualquier objeto o sistema que tenga la funcionalidad de procesar datos electrónicos o conectarse a redes informáticas, tales como: servidores físicos o virtuales, computadoras de escritorio, tabletas, dispositivos móviles, entre otros;

11. **Hardware:** Componentes físicos para tener acceso al sistema de gestión Institucional, sistemas académicos y al correo Institucional;

12. **Información confidencial:** Información personal, que no está contemplada en el principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales.

    Información que perjudique a la intimidad de la persona o cuyo uso indebido genere discriminación, revele su origen étnico, su vida afectiva y familiar, creencias religiosas, filiación o pensamiento político, condición migratoria, su vida sexual o reproductiva, su orientación sexual, identidad de género, datos biométricos, cuyo uso público atente contra los derechos humanos consagrados en la Constitución de la República e Instrumentos Internacionales;

13. **Información Crítica:** Información que se considera indispensable para la operatividad de la Universidad Estatal de Milagro (ejemplo: datos personales, información académica, bases de datos, códigos fuente, entre otros);

14. **Información Institucional:** Todo documento, físico y/o digital, generado en los activos de información institucional o por los servidores públicos de la Universidad Estatal de Milagro, en el ámbito de su competencia;

15. **Información oficial:** Toda aquella información o anuncio emitido únicamente desde los canales oficiales de la Universidad Estatal de Milagro;

16. **Integridad:** Propiedad de proteger la precisión y completitud de los activos;

17. **Mensaje de datos:** Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, e intercambio electrónico de datos;

18. **Nube:** Activo de información institucional que permite a la comunidad universitaria y a los usuarios externos autorizados, tener acceso al sistema de gestión Institucional, sistemas académicos, así como también a archivos y aplicaciones desde cualquier dispositivo;

19. **Protección de datos:** Derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información, requerirán la autorización del titular o cuando se requiera mediante petición judicial;

20. **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información;

21. **Sistemas de Información:** Conjunto organizado de recursos y procedimientos de computación y comunicación; es decir, equipos y servicios, junto con su infraestructura, instalaciones y personal de apoyo, que crean, recopilan, registran, procesan, almacenan, transportan, recuperan, exhiben, difunden, controlan o proporcionan información para realizar un conjunto de funciones;

22. **Software:** Programas de computadora (que se almacenan y se ejecutan en el hardware de la computadora) y datos asociados (que también se almacenan en el hardware físico o virtual) que se pueden escribir o modificar dinámicamente durante la ejecución;

23. **Software Malicioso:** Hardware, firmware o software que se incluye intencionalmente o se inserta en un sistema para un propósito dañino. Un programa que se inserta en un sistema, generalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de la información, datos, aplicaciones o sistema operativo de la víctima, o de molestar o interrumpir a la víctima;

24. **Usuarios de los activos de información:** Todo miembro de la comunidad universitaria, incluidos los usuarios externos que intervengan en la ejecución de los procesos de la Universidad Estatal de Milagro;

25. **Usuarios Externos:** Se consideran usuarios externos a quienes no forman parte de la comunidad universitaria, pero que, con el fin de ejecutar actividades de gestión, académicas, investigación, vinculación, auditoría, evaluación y control, requieren acceso a los activos de información de la Institución;

26. **Virus:** Software (generalmente lógica maliciosa y oculta) que se propaga al infectar; es decir, al insertar una copia de sí mismo en otro programa y convertirse en parte de este. Un virus no puede correr solo, requiere que su programa host se ejecute para activarse.

DEL USO DE LA INFORMACIÓN Y LOS ACTIVOS DE INFORMACIÓN INSTITUCIONAL

1. PROPIEDAD Y USO

Toda la información generada, desarrollada y/o contenida en los activos de información, es propiedad de la Universidad Estatal de Milagro. Se excluye la información personal de los miembros de la comunidad universitaria y usuarios externos.

Toda la información producto de las actividades administrativas y/o académicas realizadas por los miembros de la comunidad universitaria y usuarios externos en los activos de información institucionales y no institucionales, es propiedad de la Universidad Estatal de Milagro.

Toda información y activo de información institucional se utilizará para el beneficio de la Universidad Estatal de Milagro y sus dependencias.

Es responsabilidad de los miembros de la comunidad universitaria y usuarios externos utilizar adecuadamente la información y activos de información institucionales; así como suscribir los acuerdos de confidencialidad y no divulgación de la información, conforme a las directrices y procedimientos emitidos.

Es de prioridad alta la suscripción de los acuerdos de confidencialidad y no divulgación de la información por parte de los miembros de la comunidad universitaria y usuarios externos, previo al acceso a los activos de información, activos de información crítica, aplicaciones institucionales, información institucional e información crítica.

La Dirección de Operaciones Tecnológicas y de Laboratorio, deberá presentar directrices y/o procedimientos para que los activos de la información se

encuentren actualizados y asegurados a nivel de software y hardware; así también, definirá las características técnicas generales y específicas que sirvan como base para la adquisición de nuevos activos de información institucional.

El Oficial de Seguridad de la Información se encargará de la aplicación de los mecanismos definidos para la protección de la información contenida en los activos de información institucional.

El Oficial de Seguridad de la Información realizará evaluaciones periódicas a los activos de información de propiedad de la Universidad Estatal de Milagro, así como los activos rentados mediante procesos de contratación e informará al Comité de Seguridad y al Rector según corresponda, sobre los hallazgos relativos a la seguridad de la información con nivel de impacto alto; y, dará seguimiento en corto plazo a las recomendaciones que hayan resultado de cada revisión.

El uso o divulgación ilegal o inadecuada de información personal, dará lugar a las acciones legales dispuestas en la Ley Orgánica de Protección de Datos Personales, Código Orgánico Integral Penal y demás normativa legal vigente.

El uso o divulgación ilegal o inadecuada de información crítica o institucional de los activos de información institucional dará lugar a las acciones legales dispuestas en la Ley Orgánica de Protección de Datos Personales, Código Orgánico Integral Penal y demás normativa legal vigente.

No podrá acogerse a reserva, cuando se trate de investigaciones que realicen las autoridades judiciales o públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución de la República del Ecuador, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Con excepción al procedimiento establecido en las indagaciones previas.

2. DISPOSITIVOS, EQUIPOS TECNOLÓGICOS Y ELECTRÓNICOS

La Dirección de Operaciones Tecnológicas y de Laboratorios será la responsable de la administración de dispositivos, equipos tecnológicos y electrónicos, así como de la actualización del inventario, independientemente del inventario que mantenga la Gestión de Activos Fijos.

Los dispositivos, equipos tecnológicos y electrónicos institucionales se remitirán junto con un acta de entrega, en la cual se registrarán las características físicas en hardware, software y el funcionamiento de los componentes esenciales del equipo proporcionado.

La Dirección de Operaciones Tecnológicas y de Laboratorios deberá autorizar la salida de los dispositivos, equipos tecnológicos y electrónicos cuando exista la necesidad institucional. Además, será responsable de mantener un registro detallado de las solicitudes recibidas.

Es responsabilidad de los miembros de la comunidad universitaria y de los usuarios externos proteger los dispositivos, equipos tecnológicos y electrónicos institucionales que se les hayan asignado para el desempeño de sus funciones, con el fin de evitar daños o pérdidas.

3. RESPALDOS DE INFORMACIÓN

La Dirección de Operaciones Tecnológicas y de Laboratorios deberá emitir las directrices y/o procedimientos para gestionar los respaldos de los activos de información críticos e información crítica institucional.

Los respaldos de los activos de información críticos, así como de la información crítica, deberán almacenarse de manera cifrada, fuera de la Institución. Para el efecto, la Dirección de Seguridad Informática establecerá los mecanismos para definir el nivel de seguridad mínimo para el uso de cifrado de información y de contraseñas, para la protección de la información confidencial de la institución y de los datos.

Es responsabilidad de todos los miembros de la comunidad universitaria realizar los respaldos de la información generada en el ejercicio de sus actividades, utilizando la nube institucional accesible a través del correo electrónico institucional. Asimismo, corresponde a La Dirección de Operaciones Tecnológicas y de Laboratorios emitir las directrices y/o procedimientos necesarios para correcta ejecución de dichos respaldos.

4. DESTRUCCIÓN DE INFORMACIÓN

Serán destruidas las copias de seguridad/respaldos de los activos de información críticos, así como de la información crítica institucional desactualizada e innecesaria, provenientes de todas las unidades académicas y administrativas de la Universidad Estatal de Milagro.

La eliminación/destrucción de estas copias será autorizada por las autoridades académicas y administrativas, conforme al procedimiento que deberá ser emitido por el Oficial de Seguridad de la Información.

5. CLASIFICACIÓN DE LA INFORMACIÓN

Con el fin de precautelar la protección y custodia de la información contenida en documentos digitales, correos electrónicos, bases de datos, medios de almacenamiento, archivos de audio y video; e, información verbal, se establece la siguiente clasificación de la información, de acuerdo con su nivel de confidencialidad:

a) **Información Confidencial. -** Información que solo puede ser conocida y utilizada por las autoridades de la Universidad Estatal de Milagro, cuya divulgación o uso no autorizado podría ocasionar perjuicios graves de muy alto impacto o estratégicos para la Institución o terceros;

b) **Información Restringida. -** Información que solo puede ser conocida o utilizada por aquellos servidores públicos de la Universidad Estatal de Milagro para realizar su trabajo, cuya divulgación o uso no autorizado podría ocasionar perjuicios de mediano/alto impacto a la Institución o terceros;

c) **Información de Uso Interno. -** Información que puede ser conocida y utiliza por un grupo de servidores de la Universidad Estatal de Milagro que la necesiten para realizar su trabajo y entidades externas debidamente autorizadas, cuya divulgación y uso no autorizado podría incrementar el riesgo o derivar pérdidas leves a la Institución o terceros; e,

d) **Información Pública. -** Información que puede ser conocida y utilizada sin autorización por cualquier persona, ya sea, servidor público de la Institución o no.

Cada Unidad organizacional será responsable de clasificar la información bajo su custodia, de acuerdo con las disposiciones emitidas por el Oficial de Seguridad de la Información.

6. ACUERDOS DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN

El Oficial de Seguridad de la Información, remitirá los acuerdos de confidencialidad y no divulgación de la información, los cuales se emitirán de acuerdo con los niveles de responsabilidad de la comunidad universitaria y usuarios externos. Estos acuerdos deberán ser generados y actualizados según las necesidades institucionales.

Las Direcciones de: Talento Humano, Tecnología de la Información y de Comunicaciones, Seguridad Informática, Operaciones Tecnológicas y de Laboratorios y Dirección Administrativa, serán las responsables de coordinar la suscripción de los Acuerdos de Confidencialidad que deban firmarse según corresponda.

7. USO DE ANTIVIRUS

Los equipos tecnológicos de la Universidad Estatal de Milagro (UNEMI) deberán contar con un antivirus institucional actualizado, capaz de detectar y bloquear amenazas informáticas.

La Dirección de Operaciones Tecnológicas y de Laboratorios deberá realizar el monitoreo constante de las alertas emitidas por la consola de administración del antivirus y deberá responder de manera efectiva e inmediata ante cualquier incidente detectado.

La Dirección de Seguridad Informática deberá definir y supervisar los mecanismos de protección contra amenazas, identificar vulnerabilidades y evaluar la seguridad de los sistemas. Además, implementará un Programa de Concientización en Seguridad para los usuarios de la UNEMI y gestionará los incidentes ocurridos para asegurar la continuidad operativa.

La Dirección de Operaciones Tecnológicas y de Laboratorios, deberá monitorear la actualización y correcto funcionamiento del antivirus, emitir directrices para la instalación y uso adecuado del software de seguridad y responder de manera inmediata ante incidentes detectados o reportados por los usuarios.

Ambas direcciones deberán coordinar esfuerzos para garantizar la protección de los sistemas y la seguridad de la información institucional. El incumplimiento de estas disposiciones será sujeto a medidas correctivas conforme a la normativa vigente.

8. CONTROL DE ACCESO A APLICACIONES INSTITUCIONALES, SISTEMA OPERATIVO Y SISTEMAS DE GESTIÓN GUBERNAMENTAL

Todos los sistemas de información que adquiera y/o desarrolle la Universidad Estatal de Milagro, deberán contar con mecanismos de control y autenticación cifrados para su acceso, como: usuario, contraseñas, doble autenticación, registro de acceso, permisos, entre otros; siendo responsabilidad de la Dirección de Operaciones Tecnológicas y de Laboratorios la emisión de las directrices y/o procedimientos respectivos.

La Dirección de Tecnologías de la Información y Comunicaciones deberá desarrollar y/o establecer mecanismos necesarios para impedir accesos no autorizados a los sistemas de gestión académicos (aplicaciones institucionales). En caso de que la plataforma tecnológica contenga la opción de acceso como administrador al perfil de un usuario, será necesario registrar todas las actividades realizadas y generar notificaciones al usuario sobre los accesos y cambios efectuados por el administrador.

La Dirección de Operaciones Tecnológicas y de Laboratorios deberá implementar los procedimientos y configuraciones necesarias para impedir accesos no autorizados a los sistemas operativos de los dispositivos tecnológicos, a través de la aplicación de controles apropiados que permitan autenticar correctamente a los usuarios, proporcionar el acceso que les corresponda según sus perfiles y funciones, registrar sus actividades y generar notificaciones en caso de incumplimientos; como, por ejemplo: Active Directory.

La Dirección de Operaciones Tecnológicas y de Laboratorios otorgará los permisos a los sistemas de gestión gubernamental, mediante el formato definido.

9. USO DEL INTERNET

El uso del internet de la Universidad Estatal de Milagro está destinado para fines académicos, de investigación, administrativos y de vinculación; y, debe estar disponible para todos los miembros de la comunidad universitaria dentro del campus universitario.

Los dispositivos tecnológicos personales de usuarios o visitantes externos que no sean de propiedad de la institución, no deberán tener acceso a la red Wifi que es de uso exclusivo para el personal académico y administrativo de la UNEMI.

El uso de blogs, redes sociales, plataformas de video, entre otros, será limitado dentro del horario de trabajo, para que tal uso no interfiera en las labores diarias de los servidores públicos y trabajadores. El buen uso de los recursos referidos, para actividades académicas, no está restringido.

Los usuarios del servicio de internet provisto por la Universidad Estatal de Milagro, deben conocer y cumplir con las directrices y/o procedimientos establecidos por la Dirección de Operaciones Tecnológicas y de Laboratorios en relación a su uso.

Queda prohibido difundir contenidos discriminatorios, despectivos, difamatorios o acosadores, así como cualquier otro contrario a la legalidad o la ética, además el envío de mensajes no relacionados con los objetivos de la Institución, empleando la infraestructura tecnológica de la Universidad Estatal de Milagro.

10. USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

Las cuentas de correo electrónico institucional serán generadas y gestionadas por la Dirección de Operaciones Tecnológicas y de Laboratorios con el empleo de dominios válidos autorizados por la Universidad Estatal de Milagro; por lo que, a efectos de evitar eventuales riesgos ocasionados por su inadecuada utilización, se acatarán las disposiciones contenidas en la Ley de Comercio

Electrónico, Firmas Electrónicas y Mensajes de Datos, su Reglamento y demás normativa legal vigente.

Las cuentas de correo electrónico institucional serán utilizadas únicamente en asuntos relacionados con las funciones y actividades institucionalmente asignadas. Cada usuario es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte al correo electrónico institucional, así como de asegurarse de cerrar la sesión correspondiente al finalizar el uso del correo.

El uso que se dé a la cuenta de correo electrónico institucional será de responsabilidad exclusiva de su titular.

La Dirección de Operaciones Tecnológicas y de Laboratorio, deberá emitir las directrices y/o procedimientos para el uso del servicio de correo electrónico institucional.

11. REDES SOCIALES OFICIALES

La Dirección de Comunicación Institucional elaborará, actualizará y socializará un instrumento para el uso de las redes sociales oficiales.

Se deberá solicitar la creación de correos asociados a cada red social oficial de la Universidad Estatal de Milagro, información que deberá ser remitida a la Dirección de Seguridad Informática.

La Dirección de Seguridad Informática deberá crear las cuentas y configurar los equipos destinados al manejo de las redes sociales oficiales de la institución con los controles de seguridad mínimos como: manejo de contraseña, autenticación de dos factores u otras herramientas que permitan autenticar correctamente al administrador/es de la plataforma de las redes sociales oficiales, previo su entrega a la Dirección de Comunicación Institucional.

Toda red social oficial de la Universidad Estatal de Milagro, deberá estar asociada a un número telefónico institucional para doble factor de autenticación, siendo el Oficial de Seguridad de la Información custodio y responsable del uso del dispositivo tecnológico asignado para la creación y control de acceso a las redes sociales oficiales de la Institución.

La Dirección de Seguridad Informática analizará los niveles de seguridad de las plataformas sociales, políticas de seguridad: verificación de cuentas, conexiones seguras (HTTPS), gestión de permisos, uso de contraseñas seguras, opciones de privacidad, etc.

12. INSTALACIÓN DE SOFTWARE

Los softwares y aplicaciones que se instalen en los equipos de cómputo o dispositivos tecnológicos que pertenecen a la Universidad Estatal de Milagro deben contar con licencia. No está permitida la instalación de softwares o aplicaciones piratas o de dudosa procedencia.

La Dirección de Operaciones Tecnológicas y de Laboratorio deberá desinstalar todo software y/o aplicación no autorizada que se haya configurado en los equipos de cómputo o dispositivos tecnológicos de la Institución, mismo que deberá comunicarse a través de un informe técnico.

13. CREDENCIALES DE ACCESO A LOS ACTIVOS DE INFORMACIÓN INSTITUCIONAL

Las credenciales de acceso a los activos de información son personales e intransferibles y no deben ser exhibidas en sitios visibles.

La Dirección de Tecnologías de la Información y Comunicaciones notificará a la Dirección de Seguridad Informática en caso de detectar el uso inadecuado de las credenciales de acceso por parte de cualquier miembro de la comunidad universitaria o usuario externo, de conformidad con lo establecido en los acuerdos de confidencialidad y normativa legal vigente.

Cada usuario es responsable de cumplir con las disposiciones y procedimientos establecidos para precautelar la confidencialidad en el uso de credenciales institucionales de acceso a los activos de información.

La Dirección de Talento Humano se encargará de enviar a la Dirección de Seguridad Informática un listado que incluirá los servidores asignados, el cargo y sus respectivos roles, basado en las responsabilidades, funciones y/o delegaciones establecidas en la normativa interna. Esta información permitirá que la Dirección de Seguridad Informática defina, valide y apruebe los perfiles de usuario, roles de acceso por función, niveles de permiso de seguridad correspondientes. Posteriormente, dicha dirección notificará a la Dirección de Operaciones Tecnológicas y de Laboratorios para que procedan con la creación de los accesos necesarios.

En caso de que un servidor público sea separado de su cargo o cambie de unidad, la Dirección de Talento Humano notificará a la Dirección de Seguridad Informática para que realice la misma gestión mencionada en el inciso anterior.

Posterior a ello, en los casos que se requiera, se notificará a la Dirección de Operaciones Tecnológicas y de Laboratorios, para que realice el cambio en los permisos y/o roles de las plataformas institucionales que se encuentran bajo su cargo. En todos los casos mencionados, se requerirá que el servidor que reciba

perfiles de usuario, roles de acceso por función, y/o niveles de permiso de seguridad, firme un Acuerdo de Confidencialidad, que será suministrado por la Dirección de Seguridad Informática.

14. SEGURIDADES DE REDES LAN E INALÁMBRICAS

La Dirección de Operaciones Tecnológicas y de Laboratorios implementará reglas de tráfico en el firewall de borde entre la red WAN y la red LAN de la Universidad Estatal de Milagro; y, será responsable del control y monitoreo del consumo de red para identificar el uso innecesario del servicio de internet.

La comunidad Universitaria y usuario externo contarán con accesos a las redes LAN e inalámbrica para descarga de información inherentes a las actividades asignadas, conforme a las directrices y/o procedimientos emitidos.

La Dirección de Operaciones Tecnológicas y de Laboratorios deberá activar el medio de autenticación y autorización en las redes LAN e inalámbricas para mantener el acceso limitado. Además, será responsable de la segmentación de la red, para evitar accesos no autorizados a la red principal utilizada por el personal administrativo y académico de la institución, salvaguardando así la integridad del sistema y de la información.

En caso de que la red WAN, LAN o Wifi sean administradas por terceros, la Dirección de Operaciones Tecnológicas y de Laboratorios proporcionará las directrices necesarias para la segmentación de la red y solicitará la documentación de las configuraciones implementadas.

En caso de ataque cibernético deberá notificar a la Dirección de Seguridad Informática para que

15. SEGURIDADES DE REDES PRIVADAS VIRTUALES (VPN)

Toda conexión a la red de la Universidad Estatal de Milagro a través de VPN será autorizada, monitoreada y gestionada conforme a los requisitos y procedimientos establecidos por la Dirección de Operaciones Tecnológicas y de Laboratorios.

16. ACCESO REMOTO

El acceso remoto a la red institucional será otorgado a los usuarios que lo requieran para el desempeño de sus funciones, de acuerdo con los roles y responsabilidades previamente establecidos, el mismo que se concederá cumpliendo con los requisitos y procedimientos definidos por la Dirección de Operaciones Tecnológicas y de Laboratorios.

Para los usuarios externos, como proveedores, contratistas y demás entidades públicas o privadas que presten servicios a la Universidad Estatal de Milagro y requieran acceso a la red institucional, los permisos serán otorgados una vez que haya verificado las condiciones de seguridad, de conformidad con los siguientes parámetros:

a) Los accesos vía remota se realizarán exclusivamente mediante herramientas tecnológicas autorizadas y dispuestas por la Dirección de Operaciones Tecnológicas y de Laboratorios
b) Cualquier tipo de acceso remoto se realizará mediante conexiones seguras tipo VPN, SSL, IPSec, conexiones HTTPS, o conexiones cifradas;
c) La Dirección de Operaciones Tecnológicas y de Laboratorios tendrá la potestad de monitorear en todo momento las acciones que se ejecuten mediante el uso del acceso remoto;
d) Los servidores públicos de la Institución o usuarios externos que requieran utilizar una conexión remota para acceder a la red institucional, solicitarán autorización a la Dirección de Operaciones Tecnológicas y de Laboratorios. Para efectos de control, se deberá mantener un registro de las solicitudes recibidas;
e) Los accesos que se realicen vía remota se limitarán exclusivamente a aquellos recursos que se requieran para el desarrollo de las labores del servidor solicitante, de acuerdo con sus funciones, recursos que se detallarán específicamente en el formulario de solicitud; y,
f) Es responsabilidad permanente de los miembros de la comunidad universitaria y usuarios externos, proteger y resguardar sus credenciales, así como los datos proporcionados y demás información inherente a la conexión de acceso remoto que les haya sido autorizada.

17. REDES INALÁMBRICAS NO AUTORIZADAS

Está prohibida la instalación de todo tipo de dispositivos, tales como puntos de acceso, routers inalámbricos, entre otros, que no hayan sido verificados y validados por la Dirección de Operaciones Tecnológicas y de Laboratorios. En caso de detectarse dispositivos no autorizados, dicha unidad emitirá un informe técnico que comunicará la necesidad de desinstalar y retirar los dispositivos de manera inmediata.

18. USO DE LA INTELIGENCIA ARTIFICIAL

El uso de herramientas de inteligencia artificial (IA) en la Universidad Estatal de Milagro, no será restringido, pero estará sujeto a una declaración de su uso y responsabilidad. Su implementación en actividades académicas, investigativas y administrativas deberá realizarse bajo los protocolos institucionales.

El uso indebido de la IA será motivo de medidas correctivas conforme a la normativa institucional y demás regulaciones aplicables.

19. AUDITORÍA Y EVALUACIÓN DE VULNERABILIDADES

El Oficial de Seguridad de la información será responsable de verificar el cumplimiento de la presente política, así como de la implementación y evaluación de los controles definidos por el Esquema Gubernamental de Seguridad de la Información (EGSI), dar seguimiento a las recomendaciones emitidas en los informes de auditoría y evaluación de riesgos, y la aplicación de sus controles.

La Dirección de Seguridad Informática llevará a cabo auditorías y/o revisiones muestrales de forma periódica, con base al cronograma aprobado por el Rector o por solicitud de los servidores de la Universidad Estatal de Milagro, las que podrán realizarse de forma remota o in situ, dependiendo de las necesidades y requerimientos específicos de cada caso.

Al finalizar la auditoría, se generará un informe detallado con los hallazgos, recomendaciones y planes de acción que deberán ser comunicados al Rector.

20. MONITOREO DE LA SEGURIDAD DE LA INFORMACIÓN

La Dirección de Seguridad Informática será la responsable de monitorear la seguridad de los sistemas informáticos e identificar vulnerabilidades de los mismos. Además, deberán definir y regular procedimientos internos que establezcan la seguridad de la información para la continuidad operacional de la institución, definiendo la clasificación de la información institucional.

En el caso de servicios prestados, será responsable de monitorear permanentemente las actividades y accesos realizados por proveedores y terceros que presten servicios tecnológicos a la Universidad Estatal de Milagro (UNEMI). Para ello deberá:

- Supervisar periódicamente el cumplimiento de los acuerdos y procedimientos establecidos con proveedores externos.
- Exigir documentación y evidencias sobre los controles de seguridad implementados por terceros.
- Realizar auditorías o revisiones técnicas para garantizar que las actividades realizadas por terceros cumplan con los estándares de seguridad definidos por la Institución.
- Comunicar al Rector cualquier vulnerabilidad o incumplimiento detectado en la gestión tecnológica de terceros, proponiendo medidas correctivas inmediatas.

El incumplimiento de estas disposiciones será sujeto a las acciones correctivas y sanciones estipuladas en la normativa institucional vigente.

21. ACTUACIÓN FRENTE A INCIDENTES DE CIBERSEGURIDAD

Ante la detección o reporte de un incidente de ciberseguridad que comprometa la confidencialidad, integridad o disponibilidad de la información institucional, la Dirección de Seguridad Informática asumirá la coordinación técnica de la respuesta institucional, conforme a las atribuciones previstas en el Reglamento de la Estructura Organizacional por Procesos.

La Dirección de Seguridad Informática dispondrá las acciones necesarias para la identificación, análisis, contención y recuperación del incidente, así como la preservación de la evidencia digital, la evaluación del impacto y la emisión de los informes técnicos correspondientes.

La Dirección de Tecnología de la Información y Comunicaciones brindará el soporte técnico requerido para la recuperación de la infraestructura tecnológica, la restauración de servicios, la administración de respaldos y la continuidad operativa de los sistemas institucionales, en coordinación con la Dirección de Seguridad Informática.

Cuando la naturaleza o gravedad del incidente lo amerite, la Dirección de Seguridad Informática coordinará la activación del equipo institucional de respuesta, integrado por las unidades administrativas competentes, incluyendo la Dirección Jurídica y Dirección de Comunicación Institucional para la atención integral del evento.

Las comunicaciones oficiales relacionadas con el incidente serán emitidas únicamente por los canales institucionales autorizados y conforme a las directrices de la Máxima Autoridad Ejecutiva.

Finalizada la atención del incidente, la Dirección de Seguridad Informática elaborará el informe técnico correspondiente, incluyendo el análisis de causas, impacto, medidas implementadas y recomendaciones para fortalecer los controles de seguridad y prevenir la ocurrencia de eventos similares.

22. MEDIDAS CORRECTIVAS O DISCIPLINARIAS

El Oficial de Seguridad de la Información deberá notificar el incumplimiento de lo establecido en la presente política al Rector, para establecer las medidas correctivas o disciplinarias a las que hubiere lugar, de conformidad con lo establecido en la Ley Orgánica de Educación Superior; Ley Orgánica del Servicio Público; Reglamento General a la Ley Orgánica del Servicio Público; y demás normativa legal vigente.

DISPOSICIONES GENERALES

PRIMERA. - La presente política deberá estar disponible de forma permanente en la página web institucional y en el repositorio, asegurando así el acceso a todos los usuarios que requieran de los recursos y activos de información institucional.

SEGUNDA. - La Dirección de Seguridad Informática se encargará de asegurar los recursos adecuados para implementar y mantener la presente política, así como de verificar su cumplimiento y fomentar una cultura de seguridad dentro de la Institución.

TERCERA. - La Universidad Estatal de Milagro tiene propiedad sobre los bienes tecnológicos asignados para el desempeño de las funciones de sus usuarios. Por lo tanto, el Oficial de Seguridad de la Información tiene la facultad de retirar y revisar el contenido de dichos bienes en cualquier momento. Además, podrá solicitar, de manera justificada, la realización de un análisis técnico especializado. Este proceso se llevará a cabo precautelando la confidencialidad y los derechos de los usuarios, conforme a lo estipulado en la normativa legal vigente.

CUARTA. - Los Acuerdos de Confidencialidad, suscritos por la comunidad universitaria y usuarios externos, reposarán en la hoja de vida, en el expediente del proceso, así como en los contratos de servicios y convenios correspondientes. Cada Unidad Organizacional de la Universidad Estatal de Milagro tendrá la facultad de emitir acuerdos específicos de confidencialidad y no divulgación, adaptados a sus productos y servicios, los cuales estarán bajo su custodia.

QUINTA. - En caso de ataques cibernéticos, el Director de Planificación Institucional en su calidad de Presidente del Comité de Seguridad de la Información, deberá convocar al mismo a sesión extraordinaria, para que el Comité evalúe la situación y disponga la implementación de medidas correctivas necesarias para mitigar el ataque. El Oficial de Seguridad de la Información, deberá elaborar el procedimiento o plan de respuesta para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.

Además, el Comité tendrá la responsabilidad de documentar todas las acciones derivadas del incidente en un expediente. Una vez completado, este expediente deberá ser remitido a la instancia correspondiente encargada de establecer e imponer las sanciones pertinentes de acuerdo con las normativas internas.

DOCUMENTOS DE REFERENCIA

Ley de Comercio Electrónico, Firmas y Mensajes de Datos;
Ley Orgánica de acceso y Transparencia a la información Pública;
Constitución de la República;
Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024;
Esquema Gubernamental de Seguridad de la Información;
Familia de Normas Técnicas ISO/IEC 27000; y,
Otros.

FIRMAS DE RESPONSABILIDAD

	Nombre/Cargo	Firma
Elaborado por:	Oficial de Seguridad de la Información	
Revisado por:	Presidente del Comité de Seguridad de la Información	

Control de Versiones

Código:	Pol. 22
Primera versión:	14.02.2025
Última reforma:	19.10.2026
Versión:	2.00
Creado por:	Oficial de Seguridad de la Información

CERTIFICACIÓN

La Infrascrita Secretaria General (S) de la Universidad Estatal de Milagro, Certifica que, la **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD ESTATAL DE MILAGRO**, fue aprobada por el Órgano Colegiado Superior, mediante RESOLUCIÓN OCS-SO-2-2025-N°3, el 14 de febrero de 2025, y reformada mediante RESOLUCIÓN OCS-SE-19-2026-N°4, el 19 de octubre de 2026.

Milagro, 19 de octubre de 2026.



Abg. Lidia Chávez Núñez Mgtr.
SECRETARIA GENERAL (S)

