



UIEPA

Universidad Interserrana del Estado
de Puebla Ahuacatlán

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD PARA LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES

INTRODUCCIÓN

Las políticas y lineamientos de seguridad informática y de comunicaciones, son directrices que tienen como objetivo promover el buen uso y cuidado de los recursos de tecnologías de información entre personal directivo, administrativo, docente, alumnado y terceros; mediante la notificación de las medidas y normas que deben cumplir y utilizar para proteger los componentes de los sistemas informáticos de la Universidad Interserrana del Estado de Puebla Ahuacatlán.

1. OBJETIVO

Definir las políticas de seguridad informática para proteger y salvaguardar la autenticidad, integridad, disponibilidad y confidencialidad de la información institucional de la Universidad Interserrana del Estado de Puebla-Ahuacatlán (UIEPA), brindando a los usuarios la orientación en el buen uso de los sistemas y servicios informáticos.

2. ALCANCE

UNIDADES ADMINISTRATIVAS DE LA UIEPA Y PARTES EXTERNAS QUE INTERVIENEN EN EL PROCEDIMIENTO.

2.1 Personal administrativo

2.2 Personal académico

2.3 Responsable del área informática

2.4 Dirección de administración y finanzas

2.5 Alumnado

3. ACCESO FÍSICO

3.1 El centro de datos de la Universidad Interserrana del Estado de Puebla Ahuacatlán es considerada un área de acceso restringido exclusivo a personal que por sus funciones requiera acceso al mismo.

| ELABORÓ | REVISÓ/AUTORIZÓ | FECHA DE ACTUALIZACIÓN | CÓDIGO | VERSIÓN | REQUISITO(S) |
|----------------|------------------------|-------------------------------|---------------|----------------|---------------------|
| JRO | AJG/GSAM | 14 de marzo del 2023 | NA | 01 | NA |

3.2 El uso de medios extraíbles como UBS, disco externo es responsabilidad de cada usuario.

4. ACCESO LÓGICO

4.1 Para hacer uso de los recursos informáticos disponibles en la Universidad Interserrana del Estado de Puebla Ahuacatlán, se deberá realizar el acceso a los sistemas a través de una cuenta única de usuario.

4.2 No deberán existir cuentas de usuarios genéricas (usuarios agrupados bajo una sola contraseña compartida) para el uso de recursos.

4.3 Para los recursos informáticos como servicio de internet, su uso es exclusivo para temas laborales.

4.4 El resguardo de la contraseña ligada a una cuenta de usuario, es responsabilidad de la persona asignada a la misma, por lo cual, no se podrá revelar ni compartir la contraseña a un tercero.

4.5 Las contraseñas no podrán exhibirse en forma alguna, ni resguardarles en archivos sin encriptar, a fin de evitar que un sujeto externo o ajeno pueda acceder a ella.

4.6 El resguardo de contraseñas vinculadas a cuentas especiales será responsabilidad del área de tecnologías de información y proporcionará dicha contraseña en función a criterios establecidos a los usuarios de la misma.

4.7 Los accesos lógicos serán realizados a través del área informática o que asigne para este fin, así mismo establecerá los lineamientos necesarios para regular el uso de los equipos, el soporte que se preste a todos los recursos informáticos y que garantice la integridad de la información contenida en los mismos.

5. LINEAMIENTOS DEL BUEN USO DE LOS ACTIVOS INFORMÁTICOS

5.1 Los usuarios que tengan activo informático asignado de manera personal para uso de sus funciones, son los únicos responsables de su utilización, así como

| ELABORÓ | REVISÓ/AUTORIZÓ | FECHA DE ACTUALIZACIÓN | CÓDIGO | VERSIÓN | REQUISITO(S) |
|---------|-----------------|------------------------|--------|---------|--------------|
| JRO | AJG/GSAM | 14 de marzo del 2023 | NA | 01 | NA |

también de la información contenida en los mismos, por lo que debe evitar compartirlos. En caso de requerir compartirlo o prestar el activo informático, será solamente para cuestiones laborales y sin liberarlo de su responsabilidad.

5.2 Toda movilización del activo informático dentro o fuera de las instalaciones de la institución es responsabilidad del resguardante.

6. CLASIFICACIÓN DE LA INFORMACIÓN

6.1 Personal responsable de resguardo de información, debe asegurar que la información esté protegida para asegurar su integridad y confidencialidad, acorde a su clasificación. La información puede estar disponible de manera electrónica, impresa en papel, magnética, óptica y otro medio.

6.2 Cada usuario deberá hacer uso de la información a la que tenga acceso únicamente para propósitos relacionados con el cumplimiento de sus funciones, debiendo resguardar principalmente la relativa a datos personales, absteniéndose de comunicarlos a terceros sin el consentimiento expreso de la persona a la que se refieren.

6.3 Usuarios que hacen uso de información clasificada como restringida o confidencial, evitarán que sea accedida por personas no autorizadas.

6.4 Personal responsable de resguardo de información deberá realizar respaldos ya sea en la nube o desde memorias extraíbles, periódicamente con la finalidad de disponer de un medio para recuperarlos en caso de su pérdida.

7. INTERCAMBIO DE INFORMACIÓN

7.1 Usuario que intercambie información reservada y/o confidencial con personal de la UIEPA o terceras personas, debe asegurar la identidad de la persona a la que le es entregada la información, ya sea por medio físico o electrónico.

7.2 Todo convenio de la UIEPA con terceras personas para compartir información reservada y/o confidencial, deberá apegarse a las disposiciones de las leyes,

| ELABORÓ | REVISÓ/AUTORIZÓ | FECHA DE ACTUALIZACIÓN | CÓDIGO | VERSIÓN | REQUISITO(S) |
|---------|-----------------|------------------------|--------|---------|--------------|
| JRO | AJG/GSAM | 14 de marzo del 2023 | NA | 01 | NA |

reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales.

8. PROTECCIÓN CONTRA CÓDIGO MALICIOSO (VIRUS)

8.1 Todo equipo de cómputo institucional debe contar con solución antivirus definida por el área de informática de la UIEPA. Si la solución no cubre a la plataforma utilizada, el personal notificará al encargado para buscar una alternativa de solución.

8.2 Usuario que identifique una anomalía en su equipo de cómputo deberá reportarla al encargado del área de informática mediante el formato de solicitud mantenimiento preventivo y/o correctivo.

9. PRESTACIÓN DE SERVICIOS POR TERCEROS

9.1 Proveedor que proporcione servicios informáticos a la UIEPA y que tenga acceso a información reservada y/o confidencial, deberá apearse a las disposiciones de las leyes, reglamentos y demás instrumentos normativos relacionados con acceso a la información pública y protección de datos personales y contar con acuerdos de no divulgación ni uso que perjudique a la universidad.

10. SERVICIOS INFORMÁTICOS EN LA RED

10.1 Todo personal, alumnado y terceros son responsables del buen uso de los servicios informáticos institucionales alojados en nuestras instalaciones y en la nube, asignados para realizar sus funciones administrativas y académicas.

10.2 Ninguna persona debe ver, copiar, alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del responsable del equipo o del dueño de la información.

10.3 Sólo el personal del área de tecnologías de información y comunicación queda facultado para acceder a los equipos de cómputo institucionales, para:

- Ejecutar las tareas del procedimiento de mantenimiento preventivo y correctivo.
- Realizar modificaciones al sistema operativo.

| ELABORÓ | REVISÓ/AUTORIZÓ | FECHA DE ACTUALIZACIÓN | CÓDIGO | VERSIÓN | REQUISITO(S) |
|---------|-----------------|------------------------|--------|---------|--------------|
| JRO | AJG/GSAM | 14 de marzo del 2023 | NA | 01 | NA |

- Realizar una revisión de seguridad informática y descartar uso indebido (daños intencionales a información o hardware) del equipo de cómputo.

10.4 A toda persona que deje de laborar o tener relación con la UIEPA le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales.

10.5 El departamento de personal comunicará al área de informática, toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de red.

11. USO DE CUENTAS DE USUARIO O USUARIA

11.1 Toda persona que requiera acceder a servicios informáticos, como al correo electrónico institucional, requerirá de una cuenta de usuario y contraseña. Estos datos serán asignados por el responsable del servicio.

11.2 Toda solicitud de alta, baja o cambio de privilegios de cuentas de personal administrativo o docente, para acceder a los servicios informáticos debe ser realizada por el jefe inmediato o jefe de área, debidamente justificado.

11.3 Todo usuario debe actualizar la contraseña de su cuenta de acceso a los servicios informáticos de manera periódica (al menos cada 4 meses) o cuando sospeche que pueda estar comprometida.

11.4 Cuando se requiera acceder a información de un equipo de cómputo y/o cuenta de correo institucional de una persona ausente, ya sea por cuestiones de salud, por estar comisionado a actividades fuera de su área de trabajo u otro motivo no especificado, el responsable del área correspondiente deberá solicitar al encargado del área informática que se brinde el acceso al equipo y/o servicio o sistema informático para poder dar continuidad a algún proceso institucional. El personal del área informática únicamente proporcionará acceso al responsable del área correspondiente que lo haya solicitado a efecto de que sustraiga la información necesaria, dejando constancia de ello por escrito y con firma del solicitante.

| ELABORÓ | REVISÓ/AUTORIZÓ | FECHA DE ACTUALIZACIÓN | CÓDIGO | VERSIÓN | REQUISITO(S) |
|---------|-----------------|------------------------|--------|---------|--------------|
| JRO | AJG/GSAM | 14 de marzo del 2023 | NA | 01 | NA |

11.5 Si una persona deja de laborar en la institución o cambia de puesto, el jefe inmediato podrá solicitar al área informática el acceso al equipo institucional que ésta tenía asignado, el cual es concedido para que sustraiga la información pertinente.

12. MONITOREO DEL USO DE LOS SERVICIOS INFORMÁTICOS

12.1 El personal del área informática realiza periódicamente revisiones de hardware y software del activo informático institucional, para dar atención a problemas de obsolescencia y revisiones de licenciamiento. Además, se monitorean los servicios informáticos de red para administrar el uso del recurso de internet y solucionar cualquier problema detectado.

13. USO DEL CORREO ELECTRÓNICO

13.1 El correo electrónico institucional es para uso exclusivo del empleado activo administrativo y/o académico. Éste deberá ser utilizado sólo para realizar actividades relacionadas con sus funciones.

13.2 Los responsables de área o departamento deberán solicitar la creación de nuevas cuentas de correo electrónico para personal a su cargo.

13.3 La UIEPA no es garante de los contenidos expresados en texto, sonido o video, redactados y enviados mediante el correo electrónico institucional. Ante algún correo de naturaleza sospechosa, abstenerse de abrirlo y eliminarlo de inmediato, para evitar descargar algún tipo de amenaza para el equipo de cómputo asignado y para la red institucional.

13.4 Toda persona que termine la relación laboral con la UIEPA, una vez recibida la notificación de baja por parte del departamento de personal, se inhabilitará el servicio de correo electrónico.

13.5 Toda solicitud de alta, baja o cambio de un grupo de correo institucional, debe ser solicitado por el responsable del área solicitante.

| ELABORÓ | REVISÓ/AUTORIZÓ | FECHA DE ACTUALIZACIÓN | CÓDIGO | VERSIÓN | REQUISITO(S) |
|---------|-----------------|------------------------|--------|---------|--------------|
| JRO | AJG/GSAM | 14 de marzo del 2023 | NA | 01 | NA |

13.6 Queda prohibido utilizar el correo electrónico para envíos de correo basura, cadenas, mercadotecnia, religiosos, propaganda política, actos agresivos e ilegales y cualquier otro contenido no apropiado para el destinatario.

13.7 Es responsabilidad de todo usuario del correo electrónico institucional notificar al personal encargado de correos, la sospecha del uso no autorizado de su cuenta.

13.8 Es responsabilidad del usuario respaldar aquellos correos electrónicos que por su contenido considere relevantes. Así mismo, el usuario deberá depurar constantemente los mensajes y borrar aquellos que no le son de utilidad, para liberar el espacio asignado a su cuenta de correo y evitar problemas de saturación.

14. USO DEL SOFTWARE

14.1. En todos los equipos de cómputo de la UIEPA, solo se permite la instalación de software con licenciamiento vigente, ya sea de uso libre o comercial. El área de soporte técnico es la única facultada para realizar la instalación del software.

14.2. Todo elemento del personal o estudiante que instale software sin licenciamiento vigente o malicioso en equipos de cómputo de la institución, se hace único responsable de las consecuencias que esto conlleve.

14.3 Las licencias de uso de software propiedad de la UIEPA otorgan a éste el derecho de emplearlas exclusivamente en los equipos asignados, propiedad de la institución.

15. POLÍTICA PARA EL USO DE CONTRASEÑAS

15.1 Se debe proporcionar el correcto diseño y uso de nombres de usuario y contraseñas dentro del área de Informática, así como establecer un estándar para la creación de contraseñas fuertes o robustas, su resguardo y la frecuencia de cambio.

| ELABORÓ | REVISÓ/AUTORIZÓ | FECHA DE ACTUALIZACIÓN | CÓDIGO | VERSIÓN | REQUISITO(S) |
|---------|-----------------|------------------------|--------|---------|--------------|
| JRO | AJG/GSAM | 14 de marzo del 2023 | NA | 01 | NA |

15.2 Esta política incluye a todo el personal y encargado del área Informática que utilicé o sea responsable de una cuenta interna con acceso a herramientas o información confidencial, así como para consolas de operación y servidores.

16. RESGUARDO DE CONTRASEÑAS

16.1 No se deben compartir las contraseñas con ninguna persona, incluyendo asistentes o secretarías, todas las contraseñas deben ser tratadas como sensibles y confidenciales.

Recomendaciones de resguardo:

- Nunca revelar la contraseña a través de una conversación telefónica.
- Nunca revelar una contraseña a través de un correo electrónico.
- Nunca hablar de una contraseña en frente de otras personas.
- Nunca revelar la contraseña a compañeros de trabajo en vacaciones, cada quien debe tener su cuenta propia.

17. VIGENCIA

17.1 Estas políticas y lineamientos surtirán efecto a partir de su publicación.

18. OTROS

18.1 Cualquier asunto no contemplado en el presente documento, será analizado y resuelto en su oportunidad por el Comité de Tecnología de Información y Comunicación de la UIEPA.

| ELABORÓ | REVISÓ/AUTORIZÓ | FECHA DE ACTUALIZACIÓN | CÓDIGO | VERSIÓN | REQUISITO(S) |
|---------|-----------------|------------------------|--------|---------|--------------|
| JRO | AJG/GSAM | 14 de marzo del 2023 | NA | 01 | NA |

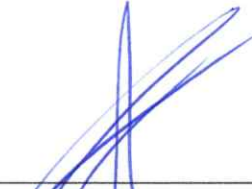
Las presentes políticas y lineamientos entran en vigor el día 14 de marzo de 2023.

Elaboró



Javier Reyes Ortega
Responsable del área informática

Revisó



Arturo Juárez García
Encargado del Despacho de la
Dirección de Planeación y Evaluación

Autorizó



Gloria Stephany Aguirre Moreno
Rectora

| ELABORÓ | REVISÓ/AUTORIZÓ | FECHA DE ACTUALIZACIÓN | CÓDIGO | VERSIÓN | REQUISITO(S) |
|---------|-----------------|------------------------|--------|---------|--------------|
| JRO | AJG/GSAM | 14 de marzo del 2023 | NA | 01 | NA |