PROTOCOLO EMERGENTE DE RECOMENDACIONES DE SEGURIDAD INFORMATICA POR LA EMERGENCIA SANITARIA OCASIONADA POR LA PANDEMIA DE COVID-19 – PRT.001

CONTENIDO

1. NORMATIVA DE REFERENCIA

Con el decreto No. No. 1017_2020 del 16 de marzo del 2020 de la presidencia de la república del Ecuador declara el estado de excepción por calamidad pública en todo territorio nacional.

Mediante Acuerdo Ministerial Nro. 00126-20201 de 11 de marzo de 2020, El Ministerio de Salud Pública declaró el Estado de Emergencia Sanitaria debido al brote del coronavirus (COVID-19).

Mediante Acuerdo Ministerial Nro. MDT-2020-076 del 12 de marzo de 2020, el Ministerio de Trabajo acuerda expedir las directrices para la aplicación del teletrabajo emergente durante la declaratoria de emergencia sanitaria.

Mediante Norma de Control Interna 410-10 de Seguridad de tecnología de información, la Contraloría General del Estado establece los siguiente 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: *"[…] 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. 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".*

Mediante Norma de Control Interna 410-11 Plan de contingencias, la Contraloría General del Estado establece los siguiente que: *"Corresponde a la Unidad de Tecnología de Información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado. Los aspectos a considerar son: […] 5. Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia. [..]".*

Mediante disposición tercera del Instructivo transitorio para la implementación de las sesiones virtuales y el teletrabajo emergente de la Unemi por la emergencia sanitaria ocasionada por la pandemia de covid-19en el cual se dispone a *"La Dirección de Tecnología de la Información y la Comunicación elaborará un protocolo con lineamientos y recomendaciones de seguridad informática institucional que será implementado en los sistemas, equipos y accesos informáticos usados por el teletrabajador".*

2. OBJETO

Este protocolo tiene por objeto poner a conocimiento de los funcionarios bajo la modalidad teletrabajo las recomendaciones de seguridad informática a ser aplicadas, hasta que culmine la declaración de emergencia sanitaria nacional, local e institucional y el estado de Excepción por motivo del covid-19.

3. ÁMBITO

El presente protocolo es de aplicación para el personal docente y administrativo acogido a la modalidad teletrabajo de la Universidad Estatal de Milagro.

4. ALCANCE

Este documento contiene las directrices que permitirán a los funcionarios ejercer sus actividades desde casa precautelando la seguridad de la información, equipos tecnológicos y accesos a las paginas institucionales gubernamentales y la red.

5. POLÍTICAS

5.1. CONFIDENCIALIDAD DE LA INFORMACION.

Dada la naturaleza de la información manejada en la institución, se debe considerar la sensibilidad de los datos que residen en los sistemas de información y equipos informáticos para el debido control y acceso. La pérdida o mal uso de esta información puede resultar en una variedad de daños, tales como pérdida de confidencialidad e incumplimiento de regulaciones y leyes aplicables a las instituciones públicas.

5.1.1. - Todo documento, carpeta u otro medio de almacenamiento que contengan información sensitiva, restringida o confidencial debe ser ubicada en áreas protegidas. Estos medios de almacenamiento de información nunca deben ser ubicados en un lugar donde visitantes pueda tener acceso a ellos.

5.1.2. - Los medios de almacenamiento que contengan información sensitiva, restringida o confidencial debe ser guardados en un área segura al final de cada día laborable.

5.1.3. - Cada usuario es responsable de asegurar todo documento y medio electrónico de almacenamiento que contenga información sensitiva o confidencial.

5.1.4. - Diversos tipos de información presentan varios riesgos. Las unidades departamentales que contengan información personal de funcionarios de la institución presten atención particular a cómo se guarda la información y otros datos sensibles. Si no

existe una necesidad legítima de información personalmente identificable, para un proceso específico no la guarde.

5.1.5. - Las impresoras deben ser localizados en áreas donde el público no pueda ver información sensitiva, restringida o confidencial.

5.1.6. - Al momento de desechar documentos físicos de carácter confidencial estos deben ser destruidos en equipos "trituradores".

5.1.7. - Las contraseñas o credenciales que permiten acceso a sistemas institucionales u otros no pueden ser apuntadas en notas ni dejadas en ubicaciones accesibles.

5.2. USO DE EQUIPOS INSTITUCIONALES.

5.2.1. - El área de tecnología será responsable de instalar los programas informáticos a ser utilizados por los funcionarios.

5.2.2. - El usuario deberá brindar condiciones físicas adecuadas para el correcto funcionamiento de los equipos tecnológicos como disponibilidad de energía, acceso a internet y temperatura ambiental adecuada.

5.2.3. - Los usuarios solo podrán utilizar los equipos institucionales para atender actividades o tareas institucionales.

5.2.4. - Queda prohibida la desinstalación del software de antivirus proveído por la institución.

6. RECOMENDACIÓN DE SEGURIDAD INFORMATICA PARA FUNCIONARIOS BAJO LA MODALIDAD TELETRABAJO.

El objeto de las presentes recomendaciones de seguridad es la de establecer un marco de principios que permitan tener acceso a la información institucional de manera segura haciendo uso de herramientas de acceso remoto, páginas webs institucionales o gubernamentales, sistemas de correos electrónicos entre otros preservando los niveles de confidencialidad de la información institucional.

Lo que permitirá lograr que la información institucional este protegido durante conducción y consecución de las actividades institucionales en la modalidad teletrabajo.

6.1. ESTABLECER CONEXIONES A INTERNET.

- Evitar conectarse a redes WIFI públicas "sin solicitud de claves de acceso".
- Si el acceso a internet de su hogar es inalámbrico procure establecer una contraseña de conexión lo suficientemente segura "letras, números y símbolos con una longitud de al menos 8 caracteres".
- Los accesos VPN serán proporcionados por el departamento de Tecnología para regular el acceso a las páginas webs institucionales y gubernamentales el funcionario será responsable de precautelar la confidencialidad de las credenciales asignadas además del uso dado a la conexión institucional.

6.2. ACCESOS A ENTORNOS WEBS

- Para el acceso a internet emplear navegadores conocidos tales como Google Chrome y Firefox evitar el uso de Internet Explorer.
- Para el ingreso a páginas webs institucionales o gubernamentales de preferencia utilizar el buscador de google.
- Antes de ingresar su usuario y contraseña en algún portal web verificar que en barra de direcciones de su navegador se anteponga https:// a la dirección web o en su defecto cuente con la imagen de un candado.

6.3. USO DEL CORREO ELECTRONICO.

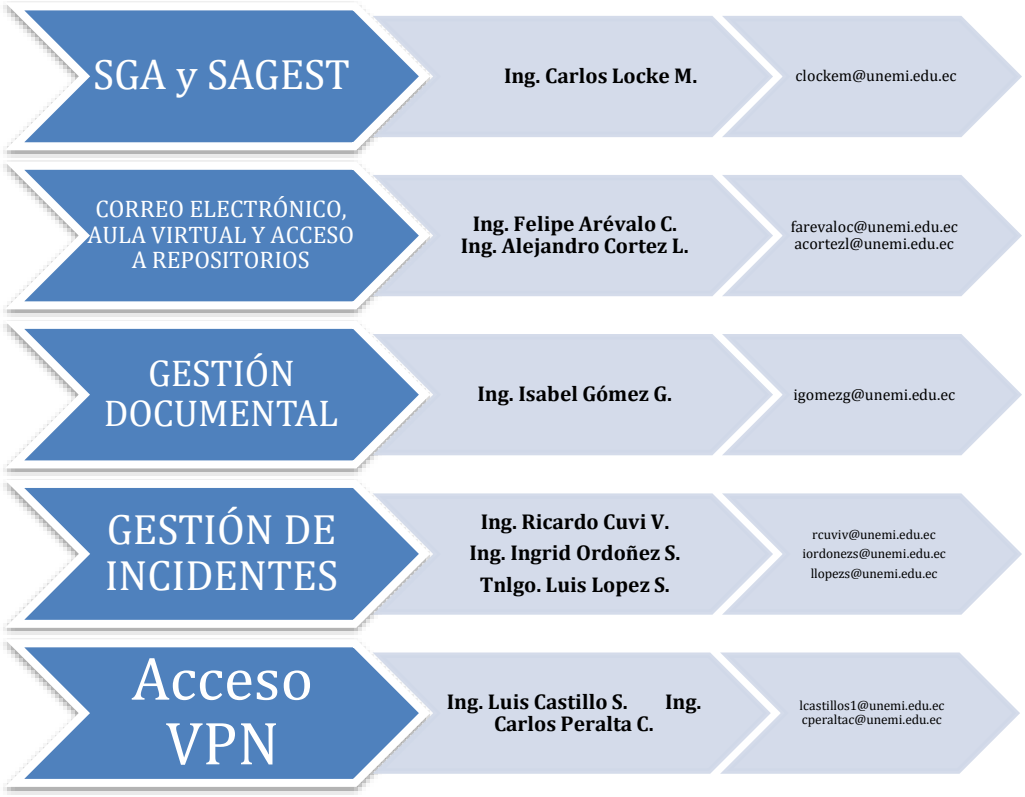
- No responda a correos electrónicos que solicitan información personal u otros en primera instancia cerciórese de la veracidad de la fuente contactando al administrador del sistema.
- No haga uso de su cuenta de correo electrónico institucional para recibir notificaciones personales o crear cuentas en páginas webs ajenas a la institución.
- El envío masivo de mails haciendo uso de listas de distribución u otros está restringido estos deberán de ser canalizados por medio del departamento Tecnología o Relaciones Publicas.

6.4. USO DEL COMPUTADOR.

- De utilizar un equipo compartido en su hogar crear una cuenta nueva específica para trabajar.
- Si su equipo le notifica acerca de una actualización de sistema operativo acéptela.
- Su computador deberá de contar con un antivirus instalado y actualizado.
- Si requiere instalar algún aplicativo cerciórese haber obtenido el mismo desde la página web del propietario.

6.5. ACCESO A SOPORTE INSTITUCIONAL.

- Las solicitudes de funcionarios que bajo la modalidad teletrabajo requiera asistencia remota por parte del departamento de Tecnología de UNEMI deberán realizarla vía mail a los siguientes correos electrónicos.



CERTIFICACIÓN

La infrascrita Secretaria General(E) de la Universidad Estatal de Milagro, CERTIFICA: Que el **PROTOCOLO EMERGENTE DE RECOMENDACIONES DE SEGURIDAD INFORMATICA POR LA EMERGENCIA SANITARIA OCASIONADA POR LA PANDEMIA DE COVID-19**, fue aprobado por el Órgano Colegiado Académico Superior, mediante RESOLUCIÓN OCAS-SO-4-2020-Nº2, el 25 de marzo de 2020.

Milagro, 3 de abril de 2020

Lic. Diana Piucay Cantillo
SECRETARIA GENERAL(E)

UNIVERSIDAD ESTATAL DE MILAGRO
7 de Febrero 2001
UNEMI
SECRETARIA GENERAL