Licenciado Leonardo Escamilla Contreras, Presidente de la Junta Directiva del Sistema Municipal para el Desarrollo Integral de la Familia del Municipio de Corregidora, Querétaro, comunico que, en Sesión Ordinaria de fecha 06 de diciembre 2022 (dos mil veintidós) la Junta Directiva del Sistema Municipal para el Desarrollo Integral de la Familia del Municipio de Corregidora, Querétaro, aprobó el siguiente ordenamiento jurídico:

LINEAMIENTOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA MUNICIPAL PARA EL DESARROLLO INTEGRAL DE LA FAMILIA, CORREGIDORA.

I.- INTRODUCCIÓN.

Con el propósito de mejorar los niveles de seguridad tanto del personal del SMDIF y de los recursos informáticos, así como de la propia información que es generada o recibida por este Organismo Descentralizado, se establecen los presentes Lineamientos en Materia de Seguridad de la información, que se detallan en el presente documento.

De igual forma y de conformidad con lo establecido en los artículos 42, fracciones IV y V de la Ley General para la Igualdad entre Mujeres y Hombres y 10 fracción III de la Ley de Igualdad Sustantiva entre Hombres y Mujeres del Estado de Querétaro, en el presente instrumento se emplea el uso de lenguaje con perspectiva de género, fomentando una imagen plural e igualitaria y no estereotipada de mujeres y hombres en Corregidora.

Para efectos del presente Instrumento, se entenderá por:

I. **Acceso Remoto:** Forma de trabajo que permite acceder a un ordenador, su interfaz y sus archivos de forma remota a través de diversas plataformas.

II. **Contralor(a):** A quien ostente la titularidad de la Contraloría del Sistema Municipal para el Desarrollo Integral de la Familia del Municipio de Corregidora, Qro.;

III. **Contraseña:** Forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso

IV. **Director(a):** A quien ostente la titularidad de la Dirección General del Sistema Municipal para el Desarrollo Integral de la Familia de Corregidora, Qro.;

V. **SMDIF Corregidora**: Al Sistema Municipal para el Desarrollo Integral de la Familia del Municipio de Corregidora, Qro.;

VI. **Internet:** Red informática de nivel mundial que utiliza la línea telefónica para transmitir la información.

VII. Ley: Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro.

VIII. Malware: Cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable.

IX. Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas

X. SSL: certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada.

XI. VPN (Virtual Private Network): Red privada virtual (VPN) que utiliza el protocolo Secure Sockets Layer (SSL)

XII. Web: Conjunto de información que se encuentra en una dirección determinada de internet.

XIII. Wifi: *'Wireless Fidelity'*, es decir,*'fidelidad inalámbrica'*. Es una tecnología de transmisión de datos inalámbrica utilizada para Internet.

II.- MARCO JURÍDICO.

1. Constitución Política de los Estados Unidos Mexicanos.
2. Constitución Política del Estado libre y soberano de Querétaro.
3. Ley Federal de Responsabilidades de los Servidores Públicos.
4. Ley de Responsabilidades Administrativas del Estado de Querétaro.
5. Ley de Archivos del Estado de Querétaro.
6. Ley de Fiscalización Superior y Rendición de Cuentas del Estado de Querétaro.
7. Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro.
8. Ley General del Sistema Nacional Anticorrupción.
9. Ley General de Responsabilidades Administrativas.
10. Ley General de Transparencia y Acceso a la información Pública
11. Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Corregidora, Querétaro.
12. Reglamento de Adquisiciones Enajenaciones Arrendamiento y Contratación de Servicios del Sistema Municipal para el Desarrollo Integral de la familia del Municipio de Corregidora, Qro.
13. Reglamento de Recursos Humanos Seguridad e Higiene del Sistema Municipal para el Desarrollo Integral de la Familia del Municipio de Corregidora, Querétaro.
14. Reglamento Interior del Sistema Municipal para el Desarrollo Integral de la Familia del

Municipio de Corregidora, Qro.

15. Decreto por el que se crea el Sistema Municipal para el Desarrollo Integral de la Familia del Municipio de Corregidora Qro.
16. Decreto por el que se reforma y adiciona diversas disposiciones del Decreto que crea el Sistema Municipal para el Desarrollo Integral de la Familia del Municipio de Corregidora Qro.
17. Código de Ética.

III.- SUJETOS DE LINEAMIENTO.

Los presentes lineamientos son de observancia general y obligatoria el personal adscrito a las Coordinaciones y Unidades que integran el SMDIF Corregidora. La inobservancia, en lo conducente, de los presentes lineamientos será causal de las responsabilidades administrativas, civiles o penales que correspondan.

IV.- LINEAMIENTOS

ACCESO FISICO

1. El área donde se localizan las fuentes eléctricas, el equipamiento y/o tableros eléctricos son consideradas áreas de acceso restringido. Será responsabilidad del encargado de la Operación de Tecnologías de la Información, establecer un control de acceso físico al interior de las mismas.

2. El SMDIF Corregidora deberá contar con un sistema de alarma ante caso de incendio o sismo que permita la coordinada evacuación del personal que labora al interior de manera eficiente.

3. El personal que labore al interior de las áreas restringidas deberá seguir los lineamientos y normas de evacuación estipuladas por la Dirección de Protección Civil del Municipio de Corregidora.

ACCESO LOGICO

4. Para hacer uso de los recursos informáticos disponibles del SMDIF Corregidora, cada uno de los trabajadores con computadoras asignadas deberá realizar el acceso a los sistemas a través de una cuenta única de usuario, existiendo una relación única entre el sujeto y su cuenta, esto a fin de autenticar al sujeto, será la responsable de administrar la información que genere.

5. Se debe establecer los mecanismos para la protección y los derechos de acceso a los recursos (sistemas informáticos y Datos) con el fin de controlar el acceso de sujetos

(Programas, procesos o usuarios), así como la utilización de los mismos, garantizando la confidencialidad e integridad de dichos recursos.

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

7. Para los recursos informáticos como servicio de internet, su uso es exclusivo para temas laborales quedando prohibido por seguridad su uso para accesos de temas que fomenten la discriminación, pornografía y sitios catalogados con contenido de tipo malicioso (malware).

8. 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, cada servidor público resguardara la contraseña impresa en un sobre cerca de la computadora y dará aviso de su ubicación a su jefe inmediato en caso de que se tenga que ausentar por horas, días o por vacaciones.

9. 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.

10. La cuenta de usuario deberá inhabilitarse de manera temporal después de un número de intentos consecutivos fallidos predeterminado por parte del sujeto, el cual intenta autenticarse a los recursos.

11. El resguardo de contraseñas vinculadas a cuentas especiales será responsabilidad de la Dirección General a través del operador técnico y proporcionará dicha contraseña en función a criterios establecidos a los usuarios de la misma (sujetos).

12. Los accesos físicos serán realizados a través de los equipos que la Dirección asigne para este fin.

A) Acceso Remoto

I. Todo acceso de un sujeto a los recursos de manera remota desde cualquier lugar deberá ser a través de una conexión segura por Internet (VPN).

II. Se deberá controlar el acceso de sujetos a los recursos a través de un túnel creado en Internet con el uso de una aplicación (Virtual Private Network), así como de la cuenta de usuario asignada al sujeto. Sera responsable del acceso remoto el técnico en informática del control y administración de usuario de acceso remoto.

B) Puesto de trabajo

I. Los equipos o terminales que no registre actividad por un periodo máximo de 10 minutos, éstas deberán desactivarse a través de un “protector de pantalla”.

II. La activación de los equipos o terminales deberá ser por medio de contraseña.

III. El Analista de Soporte Técnico deberá procurar que los equipos o terminales utilizadas para realizar las funciones de los usuarios tengan contraseña de arranque, configuradas fungiendo como administrador.

IV. Todos los equipos del SMDIF Corregidora, contaran con un protector de pantalla determinado y autorizado por la Dirección General.

AUTENTICACIÓN

13. Se deberá establecer la validación o autenticación como mecanismo para permitir o denegar el acceso a los sistemas, así como para negar una transacción proveniente de alguien no autorizado.

14. El proceso de validación deberá minimizar las falsas aceptaciones o entradas no autorizadas a los sistemas, así como los falsos rechazos, esto mediante la utilización de mecanismos autenticación (contraseña, credenciales, etc.) para lograr el acceso a los sistemas.

15. Para verificar la identidad del sujeto y por lo tanto ganar el acceso a los recursos como sujeto autorizado, deberá existir una cuenta única de usuario vinculada al sujeto, es decir, existirá una relación única entre la persona y su cuenta.

16. Para fortalecer el método de autenticación por contraseña deberá observarse lo siguiente:

a. La contraseña será construida con una longitud de al menos de ochocaracteres.
b. La construcción será una mezcla aleatoria de caracteres alfabéticos,especiales y numéricos.
c. Los caracteres alfabéticos utilizarán mayúsculas y minúsculas.
d. La construcción no partirá de lo siguiente: Una palabra común del lenguaje ode la jerga, el nombre del sujeto o usuario, pariente o de la información personal del usuario (número telefónico, número de identificación, fecha denacimiento, etc.)
e. La contraseña construida será significativamente diferente respecto de otras contraseñas anteriormente creadas (relación de caracteres utilizados).

17. Se deberá establecer los métodos apropiados de autenticación remota (conexión) a través de del intercambio de credenciales para cada una de las partes en la conexióna fin de autenticar al sujeto y establecer la conexión segura.

AUTORIZACIÓN E INTEGRIDAD

18. Para la utilización de los recursos por parte de los usuarios, se debe establecer diferentes niveles de autorización (solo podrán autorizar los titulares de las áreas de primer nivel del SMDIF Corregidora) con el objeto de poder realizar operaciones sobre los recursos con derecho de acceso.

19. Los privilegios asignados a un sujeto para ejecutar ciertas operaciones sobre los recursos deberá basarse en los derechos de acceso (protección) sobre cada recurso.

20. Se debe implantar los controles para prevenir el acceso no autorizado de terceros a los datos sensibles del SMDIF Corregidora con el fin de garantizar la confidencialidad, no repudio y la integridad de la misma, debido a las vulnerabilidades existentes en el uso de conexiones públicas o datos sin codificación, contraseña, y accesos al Wifi e Internet.

CLASIFICACIÓN DE INFORMACIÓN

21. Toda la información contenida en equipos a cargo del SMDIF Corregidora deberá estar clasificadasiguiendo los lineamientos que se han establecidos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro.

22. La Contraloría a través de la Unidad de Acceso a la Información será la responsable de solicitar a las áreas propietarias de la información la clasificación de la misma para que esta sea informada y resguardada por el área técnica y se tomen las medidas de protección pertinentes.

CONFIDENCIALIDAD

23. Todos los servidores públicos, personal de honorarios, becarios o proveedores adscritos al SMDIF Corregidora, deberán firmar una responsiva de confidencialidad donde se comprometan a mantener de manera confidencial la información que tienen a su cargo.

24. No está permitido hacer referencia a temas o información oficial y confidencial del SMDIF Corregidora en público o la distribución de mismos por medio de cualquier dispositivo o canal de comunicación no controlados.

25. La información sensible transferida a cualquier dispositivo móvil (laptops y tablets) debe estar cifrada de acuerdo a los lineamientos establecidos, a las leyes y reglamentos

correspondientes.

26. Los usuarios con capacidad de acceso remoto a través de VPN asumen la responsabilidad del buen uso de este recurso y deberán tomar las medidas de prevención adicionales para asegurar el adecuado manejo de los recursos sensibles.

27. La información sensible almacenada en equipos personales del SMDIF Corregidora, deberá estar cifrada o cuando ésta sea copiada, asimismo la información sensible transmitida a través de redes públicas será enviada de manera cifrada.

28. Los equipos virtuales establecidos como estratégicos deberá sujetarse a la presente políticas de cifrado de la información.

29. Los mecanismos de la tecnología de cifrado deberán configurarse de acuerdo a las mejores prácticas de acuerdo a los marcos de referencia existentes, garantizando la efectividad contra posibles violaciones.

30. El Analista de Soporte Técnico deberá determinar las siguientes condiciones en cuanto al cifrado de información:

I. Identificar la información o grupo de datos sensibles del SMDIF Corregidora para su cifrado con autorización de la Dirección General y/o titulares del área, debiendo hacer del conocimiento a la Contraloría.

II. Grupo de sujetos especiales con acceso o manejo de información sensible candidatos a cifrar la información de sus equipos personales.

III. Las claves de cifrado estarán al resguardo del área técnica y cualquier solicitud de cambio para dicha clave será bajo los criterio establecidos por los titulares del área.

TRANSFERENCIA DE INFORMACIÓN

31. Deberán existir mecanismos para evitar el envío de información sensible por parte de los sujetos a fin de identificar, supervisar y proteger los mismos, y de esta manera prevenir el uso no autorizado y la transmisión de información sensible.

32. Los medios de comunicación, es decir, los enlaces de datos de las redes privadas del SMDIF Corregidora deberán de establecer mecanismos entre locaciones con el fin de cifrar el medio.

33. Las aplicaciones y portales que el SMDIF Corregidora ofrece a los usuarios internos y a

la ciudadanía serán cifrados obligatoriamente a través de certificados SSL el cual se obtendrá por medio de una entidad certificadora interna y/o externa.

INCIDENTES DE SEGURIDAD

34. Los eventos de seguridad deberán ser registrados y monitorizados, examinando los registros en bitácora de indicadores de actividades no autorizadas relacionadas con la seguridad, de esta manera, ayudando a proteger la información sensible y a través de un análisis cuidadoso de tendencias, identificar mejoras al programa de gestión de la seguridad.

35. La violación de los lineamientos de uso de los recursos informáticos de la SMDIF Corregidora constituye un incidente de seguridad que deberá de ser tratado de acuerdo a la Ley de Responsabilidades Administrativas del Estado de Querétaro.

36. Se deberá contar con un procedimiento de eventos de seguridad para reunir los datos de los eventos, de las amenazas y de los riesgos, así como la revisión de dichos registros para proporcionar:

- Información sobre la seguridad.
- Lograr respuestas rápidas a los incidentes.
- Gestionar los registros almacenados.
- Generar reportes de cumplimiento.

37. El objeto del proceso de eventos de seguridad deberá ser el de encontrar eventos correlacionados, tales como:

- Acceso individual a la información sensible.
- Todas las acciones realizadas por cuentas privilegiadas.
- Acceso a los datos y funciones de la auditoria.
- Intentos inválidos de accesos lógicos.
- Todas las acciones de identificación y autenticación.
- Creación y eliminación de objetos a nivel del sistema.

Asimismo, del aprendizaje obtenido, las posibles acciones incluyen:

- Aplicar los controles apropiados.
- Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios del SMDIF Corregidora para la aceptación de riesgos.
- Evitar los riesgos.
- Transferir a otras partes los riesgos asociados con las actividades de la organización,

por ejemplo: aseguradoras y proveedores.
Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.

- Se deben seleccionar e implantar los objetivos de control, así como los controles para cumplir con los requerimientos identificados en el proceso de valoración y tratamientode riesgos.

PROVEEDORES EXTERNOS

38. Todas las áreas que contraten servicios administrados al interior del SMDIF Corregidora deberán garantizar que los contratos correspondientes tiene definido de manera clara los niveles de servicio que serán otorgados, así como las penalizaciones en caso de incumplimiento de los mismos.

39. Todos los contratos con proveedores externos deberán contener cláusulas de confidencialidad que obliguen al personal en sitio el mantener la confidencialidad, integridad y disponibilidad de la información al interior del SMDIF Corregidora.

40. Todos los contratos con proveedores externos deberán contener una cláusula que garantice que el personal asignado del SMDIF Corregidora, no tiene antecedentes penales o que superfil lo vuelve apto para desempeñar las funciones conferidas.

41. Todos los contratos con proveedores externos deberán contener una cláusula que permita imponer penalizaciones hasta la recisión del contrato en caso de que el personal de dicho proveedor se vea involucrado en un incidente de seguridad que sea catalogado como de alto riesgo.

RESPALDOS DE INFORMACIÓN

42. El Analista de Soporte Técnico del SMDIF Corregidora será responsable de llevar a cabo el respaldo de toda la información contenida en los equipos de procesamiento central a cargo del SMDIF Corregidora.

43. Los respaldos deberán hacerse con la periodicidad necesaria que minimice en medida de lo posible la posibilidad de pérdida de información en caso de alguna fallao caso fortuito.

44. Los respaldos deberán resguardarse en duplicado manteniendo un juego en el centro de datos y otro fuera del mismo para minimizar la posibilidad de pérdida de información en caso de un sismo.

BORRADO DE INFORMACIÓN

45. El Analista de Soporte Técnico del SMDIF Corregidora será responsable de proveer el software necesario para llevar a cabo el borrado seguro de información de la infraestructura física cuando ésta deje de operaro sea retirada del Centro de Datos, en cumplimiento a lo establecido en los lineamientos generales aplicables.

46. El Analista de Soporte Técnico del SMDIF Corregidora será responsable de ejecutar el borrado seguro de los equipos con el software proporcionado y guardar los certificados que demuestren el proceso, mismos que podrán ser requeridos en caso de auditoría o investigación porincidente de seguridad.

T R A N S I T O R I O S

PRIMERO. Publíquese en la Gaceta Municipal de Corregidora “La Pirámide” por una sola ocasión.

SEGUNDO. Los presentes lineamientos entrarán en vigor al día siguiente de su publicación en la Gaceta Municipal de Corregidora “La Pirámide”.

TERCERO. Se derogan todas aquellas disposiciones legales de igual o menor jerarquía que contravengan el presente Reglamento.

CUARTO. Se instruye la notificación de los presentes lineamientos a cada una de las Coordinaciones y Unidades así como la Procuraduría para informar a su personal.

QUINTO. Se instruye al Analista de Soporte Técnico elaborar los instrumentos correspondientes para dar cabal cumplimiento a lo establecido en los lineamientos, debiendo de informar de ello a la Dirección General, Coordinación de Administración y Finanzas así como marcar copia a la Contraloría.

Así lo aprobó en sesión ordinaria, la Junta Directiva del Sistema Municipal para el Desarrollo Integral de la Familia del Municipio de Corregidora, en cumplimiento a los artículos 8 fracción V y 37 fracción I del Reglamento Interior del Sistema Municipal para el Desarrollo Integral de la Familia del Municipio de Corregidora, en El Pueblito, Corregidora a los 06 de diciembre del año 2022(dos mil veintidós), por lo que:

LO TENDRÁ ENTENDIDO EL CIUDADANO PRESIDENTE DE LA JUNTA DIRECTIVA DEL SISTEMA MUNICIPAL PARA EL DESARROLLO INTEGRAL DE LA FAMILIA DEL MUNICIPIO DE CORREGIDORA, QRO Y MANDARÁ SE PUBLIQUE Y OBSERVE.

Lic. Leonardo Escamilla Contreras.
Presidente de la Junta Directiva del Sistema
Municipal para el Desarrollo Integral de la
Familia del Municipio de Corregidora
Rúbrica

Lic. Alejandro Fayad Díaz.
Secretario de la Junta Directiva del Sistema
Municipal para el Desarrollo Integral de la
Familia del Municipio de Corregidora
Rúbrica