SECRETARÍA DE SEGURIDAD PÚBLICA DEL ESTADO DE OAXACA
CENTRO DE CONTROL, COMANDO Y COMUNICACIÓN C4

Capítulo	**6. Operaciones**	**Subcapítulo**	**6.8 Sistemas de computadoras**
Número de directiva /Referencia CALEA		**Fecha de elaboración**	**Fecha próxima revisión**
		Abril 2020	Mayo 2020
6.8.1 Observar Derechos de Autor(M)		**Revisión:**	
		1	
Alcance		Centro de Control, Comando y Comunicación C4	
Autoriza		**Ing. Enrique Quinto Ceballos Aradillas** Director General del Centro de Control, Comando y Comunicación.	

FUNDAMENTO LEGAL

1.- Constitución Política De Los Estados Unidos mexicanos.
2.- Constitución Política Del Estado Libre Y Soberano De Oaxaca
3.- Ley Orgánica Del Poder Ejecutivo Del Estado De Oaxaca
4.- Ley General Del Sistema Nacional De Seguridad Pública
4.- Ley Del Sistema Estatal De Seguridad Pública De Oaxaca
5.- Reglamento Interno De La Secretaría De Seguridad Pública.
6.- Ley Federal de derechos de autor. Capítulo IV De los Programas de Computación y las Bases de Datos. Art. 101 al 114

OBJETIVO

El objetivo de la presente Directiva es brindar los lineamientos necesarios para garantizar que los sistemas informáticos propietarios que se utilizan en las actividades diarias del Centro de Control, Comando y Comunicación (C4) de la Secretaría de Seguridad Pública de Oaxaca cuentan con las licencias correspondientes y son utilizados de acuerdo a las leyes de derechos de autor.

DESARROLLO DE LA DIRECTIVA

Para evitar responsabilidades civiles y con base en los lineamientos que se establecen en la Ley Federal de Derechos de Autor se requiere que los sistemas informáticos o tecnológicos que se utilizan en los equipos de cómputo, servidores, sistemas de radiocomunicación, telefonía o cualquier otra herramienta digital utilizada en el Centro de Control, Comando y Comunicación o en los subcentros adscritos al mismo y que tengan la necesidad de una licencia para su operación, deberán ser adquiridas de forma legal y legítima, por lo que se debe seguir con el siguiente proceso de adquisición:

a) Compra de licencias:

1. Anualmente cada una de las áreas pertenecientes al Centro de Control. Comando y Comunicación C4 deberá realizar un listado con las necesidades de adquisición y/o actualización en materia de Licenciamiento de Software, para que se registre en una bitácora de necesidades de Software, cada una de las áreas informará a la Dirección General del C4 con copia a su Director o Jefe de área mediante tarjeta informativa para conocimiento.

2. La Dirección de la Red, Voz, Datos e Imagen por medio de la Coordinación de Soporte Técnico y Desarrollo Tecnológico mantendrá al día un concentrado de licencias de las que se dispone, sus vigencias y necesidades nuevas de licenciamiento, además del área que lo requiere con su justificación y/o fundamentación operacional realizado por el área solicitante, para proyectar en un análisis anual los requerimientos reales de todas las áreas en materia de software de tal forma que se incluyan en el proyecto de compra del año siguiente.

3. Después de realizado el análisis previamente señalado, se reunirá la información de todas las áreas y se comunicará mediante tarjeta informativa a la Dirección General del C4 así como al área de compras quien habrá de realizar la gestión necesaria a través de los mecanismos autorizados; para el proceso de actualización de la información que se envía para la compra de artículos a través del Fondo de Aportaciones para la Seguridad Pública (FASP), programa mediante el cual se proveen los recursos económicos para la compra de equipo y necesidades de las corporaciones policiacas mexicanas.

4. Todas las propuestas de adquisición de licenciamiento deben contar con la autorización de la Dirección General del C4 así como del comité de análisis del área de compras quienes serán los encargados de realizar el proceso de licitación con las áreas correspondientes de la Secretaria de Seguridad Publica y de informar el resultado de las licitaciones a las áreas solicitantes.

b) Uso de licencias:

1. Una vez que el proceso de compra se haya realizado y que el proveedor proporcione la información del licenciamiento solicitado se llamará al área de compras del C4 quien en conjunto con personal del área de desarrollo tecnológico realizará la verificación de que el licenciamiento que se recibe es el que se solicitó al inicio de la licitación.

2. En caso de que todo se reciba de forma adecuada el área de compras de C4 firmará de recibido en conjunto con el Director General del C4 quien será el responsable de los materiales o licencias hasta el momento que se entregan al personal o área que los utilizará.

3. Estos materiales y licencias quedarán en resguardo del Almacén del C4 hasta el momento de su entrega.

4. Cuando el almacén haya dado de alta los materiales y licencias recibidos en el sistema de inventario entregará esta información en conjunto con el área de compras del C4 a las áreas que manifestaron sus necesidades de licenciamiento de software para que puedan realizar la instalación en los equipos que sean requeridos.

5. Cada área solicitante mantendrá un listado actualizado con las licencias restantes que tienen en su resguardo de manera que si fuera necesario podrían entregarse a otra área sin necesidad de realizar un nuevo proceso de licitación.

c) Actualización de licencias.

1. Cuando se requiera la actualización de las licencias con las que se cuenta en las instalaciones del C4 por alguno de los siguientes casos:

   - Actualizaciones necesarias del proveedor.
   - Expiración de la licencia.

   Cada área habrá de comunicar con un mínimo de seis meses de anticipación de esta situación al área de compras del C4 quien lo tomará en cuenta para los nuevos procesos de adquisición.

2. Esta situación será repetida por todas las áreas de C4 que cuenten con equipos tecnológicos que requieran de licenciamiento para su funcionamiento.

3. Una vez reunido el número de licencias que deberán ser actualizadas se seguirá el mismo procedimiento para la adquisición de licencias sólo que se hará bajo el concepto de renovación de licenciamiento.

d) Software libre.

1. En caso de que alguna licencia pueda ser sustituida por la instalación de software libre, es decir que no requiera de la compra de un licenciamiento, esta se realizará en un proceso progresivo para que los usuarios puedan adaptarse a la utilización de estas nuevas tecnologías. Esto aplicará siempre que el software propietario en cuestión pueda ser sustituido por una versión libre y que esta acción no tenga consecuencias en la operatividad de la infraestructura tecnológica del C4.

RESPONSABLES

- El Director del Centro de Control, Comando y Comunicación es el responsable de autorizar las Directivas.
- La persona designada como Gerente de Acreditación, difunde con el personal del Centro de Control, Comando y Comunicación la autorización de cada Directiva y supervisa que se cumplan con los lineamientos y procedimientos establecidos en las mismas.
- El personal del Centro de Control, Comando y Comunicación tiene la obligación de respetar y acatar la directiva así como de proporcionar la información que les solicita.

- El personal del área de compras del C4 tiene la obligación de realizar en tiempo y forma los procedimientos descritos en la directiva.

Ing. Enrique Quinto Ceballos Aradillas
Director del Centro de Control, Comando y Comunicación C4
AUTORIZÓ

Lic. Osvaldo Alejandro Hernández León
Director de la red, voz, datos e imagen del Centro de Control, Comando Y Comunicación
REVISÓ

SECRETARÍA DE SEGURIDAD PÚBLICA DEL ESTADO DE OAXACA
CENTRO DE CONTROL, COMANDO Y COMUNICACIÓN C4

Capítulo	**6. Operaciones**	**Subcapítulo**	**6.8 Sistemas de computadoras**
Número de directiva /Referencia CALEA		**Fecha de elaboración**	**Fecha próxima revisión**
		Mayo 2020	Mayo 2020
6.8.2 Virus de Computadoras (M)		**Revisión:**	
		1	
Alcance		Centro de Control, Comando y Comunicación C4	
Autoriza		**Ing. Enrique Quinto Ceballos Aradillas** Director General del Centro de Control, Comando y Comunicación.	

FUNDAMENTO LEGAL

1.- Constitución Política De Los Estados Unidos Mexicanos.
2.- Constitución Política Del Estado Libre Y Soberano De Oaxaca
3.- Ley Orgánica Del Poder Ejecutivo Del Estado De Oaxaca
4.- Ley General Del Sistema Nacional De Seguridad Pública
4.- Ley Del Sistema Estatal De Seguridad Pública De Oaxaca
5.- Reglamento Interno De La Secretaría De Seguridad Pública.

OBJETIVO

El objetivo de la presente Directiva es brindar los lineamientos necesarios para garantizar que los equipos de cómputo que se utilizan en las actividades diarias del Centro de Control, Comando y Comunicación (C4) de la Secretaría de Seguridad Pública de Oaxaca así como de los subcentros del mismo en el interior del estado cuentan con un software antivirus con las características necesarias para evitar la propagación de virus de computadoras o la violación de las políticas de seguridad de la información y archivos generados en las actividades diarias del C4.

DESARROLLO DE LA DIRECTIVA

La generación de información en forma electrónica es una de las tareas primordiales que se llevan a cabo en las instalaciones del Centro de Control, Comando y Comunicación de la Secretaría de Seguridad Pública de Oaxaca, y para su elaboración se utilizan sistemas informáticos y tecnológicos los cuales deben estar protegidos de amenazas informáticas o humanas que pudieran provocar la pérdida o alteración no deseada de la información altamente sensible que se genera a diario en las instalaciones, por lo que la Dirección de la Red, Voz, Datos e Imagen a través del departamento de Desarrollo Tecnológico deberá seguir una serie de protocolos y procedimientos para garantizar la seguridad e integridad de la información.

1. **Instalación y mantenimiento de infraestructura de Seguridad Física y perimetral:**

    a. El departamento de Desarrollo Tecnológico tendrá a su cargo la administración de la infraestructura física de seguridad informática la cual se utilizará para prevenir incidentes informáticos en las instalaciones del C4 y en las diferentes oficinas que reciban información o servicios por parte de la Secretaría de Seguridad Pública. Las políticas de seguridad del equipo

físico se deberán revisar mensualmente y se deberá llevar una bitácora de los incidentes que se generen en eso lapso de tiempo.

b. Una vez realizada la revisión mensual de las políticas éstas se ajustarán de acuerdo al resultado del análisis de seguridad que realice el personal del área de seguridad informática para ajustarlas a las nuevas necesidades tecnológicas y los requerimientos operativos por parte de las diferentes áreas que conforman el C4.

c. Entre las actividades a tener en cuenta en este apartado se pueden mencionar la gestión y actualización de los sistemas físicos cada seis meses para garantizar que se encuentren al día con las últimas actualizaciones de seguridad por parte de las empresas que brindan el servicio, así como de la vigencia del licenciamiento.

d. Cada tres meses de deben realizar revisiones del espacio físico donde se encuentran ubicados los equipos, a fin de descartar posibles fallos físicos en las instalaciones que pudieran provocar una o más fallas en los equipos tecnológicos que se encuentra en esa área, además de verificar que el espacio dedicado a la seguridad física se encuentra libre de equipos de otras áreas, o de material no utilizado que pudiera obstaculizar el paso en caso de que llegara a ser necesario la realización de actividades en el área que ocupan la Estructura Principal de Distribución (MDF, Main Distribution Frame) y la Estructura de Distribución Intermedia (IDF, Intermediate Distribution Frame) ubicados en el edificio del C4.

e. En caso de que las revisiones dieran como resultado la realización de movimientos de equipo o requerimientos de mantenimiento, estos deberán ser comunicados a la Dirección General así como a la Dirección de la red, voz, datos e imagen con al menos dos semanas de anticipación; esto para poder comunicar a otras áreas con un tiempo considerable de las posibles afectaciones que pudieran ocurrir como resultado de las operaciones a realizar.

f. Si fuera requerida la actualización de los equipos físicos o cambios en el licenciamiento esto deberá ser informado a la Dirección General con al menos tres meses de anticipación para poder contemplar las posibles acciones a realizar.

2. **Instalación y mantenimiento de software antivirus.**

a. El Centro de Control. Comando y Comunicación C4 Oaxaca debe contar en todo momento en sus equipos de cómputo y servidores con software antivirus licenciado o libre de acuerdo a las áreas operativas donde será instalado; en caso de que sea utilizado software licenciado se deben contar las licencias legítimas y originales tal y como se señala en la directiva 6.8.1.

b. El personal designado del área de soporte técnico y desarrollo tecnológico que tenga a su cargo el mantenimiento de los equipos de cómputo del centro estatal de emergencias, áreas administrativas y operativas del C4 debe realizar la verificación cada tres meses de las actualizaciones disponibles para el software antivirus que utilicen los equipos de cómputo del C4.

c. En caso que sea necesaria una actualización mayor en los equipos o el cambio de proveedor de software antivirus, esto deberá ser notificado a las áreas donde se realizará la acción a través de tarjeta informativa con copia a la Dirección General del C4 con un tiempo de 15 días antes en caso

de ser una actualización o cambio menor, y de 48 horas antes en caso de que se trate de un cambio mayor.

d. Si por motivos de seguridad u operatividad es necesario realizar el cambio de forma inmediata, ésta se podrá realizar previa autorización de la Dirección General del C4 informando de forma escrita posteriormente al encargado del área donde se realizó el cambio a través de una tarjeta informativa.

e. En caso de que el personal del área de soporte técnico y desarrollo tecnológico durante sus revisiones programadas encuentre que algún equipo cuenta con más de un software antivirus instalado se procederá la eliminación del mismo para evitar redundancia, informando de esta acción al Director de la red, voz, datos e imagen con copia al Director del C4 y al encargado del área donde se encontró la situación señalada a través de tarjeta informativa.

3. **Atención a situaciones de riesgo.**

Aun cuando se lleven a cabo las mejores prácticas y se sigan los protocolos de actualización y mantenimiento del software antivirus, es posible que se presenten brechas de seguridad y riesgos informáticos los cuales se atenderán de la siguiente manera:

a. Alertamiento por infección de virus de computadoras:
Cuando algún equipo informático presente disminución de su rendimiento y la causa probable determinada por el personal del área de soporte técnico y desarrollo tecnológico sea la infección de un virus de computadora, se procederá a realizar la eliminación del mismo siempre que esto sea posible aislando el equipo en cuestión en un área de servicio desconectado de la red interna del C4 para evitar la propagación del mismo.

Si el virus no puede ser eliminado de forma permanente se procederá a realizar el respaldo de la información del equipo y se realizará un mantenimiento correctivo completo, entregando el equipo nuevamente en perfectas condiciones. Posterior a este procedimiento se deberá informar al encargado del área de donde procede el equipo a través de tarjea informativa para conocimiento de las acciones realizadas.

4. **Capacitación al personal en temas de seguridad informática.**

a. Por lo menos una vez cada seis meses se deberá realizar una junta con el personal operativo del C4 y enviar la información de la reunión a los subcentros donde se expliquen los riesgos informáticos que estén propagándose en el momento de la reunión procurando en todo momento de informar las consecuencias que se presentarían a la integridad de la infraestructura física y a la información generada en caso de que llegara a presentarse un caso de virus informático en las instalaciones.

b. Informar al personal de las acciones que deben realizar en caso de que se presente alguna falla de seguridad en sus equipos de trabajo, así como a quien deben reportar esta situación señalando que se debe realizar de forma inmediata para prevenir mayores consecuencias.

RESPONSABLES

- El Director del Centro de Control, Comando y Comunicación es el responsable de autorizar las Directivas.
- La persona designada como Gerente de Acreditación, difunde con el personal del Centro de Control, Comando y Comunicación la autorización de cada Directiva y supervisa que se cumplan con los lineamientos y procedimientos establecidos en la misma.
- El personal del Centro de Control, Comando y Comunicación tiene la obligación de respetar y acatar la directiva así como de proporcionar la información que les solicita.
- El personal designado de la Dirección de la Red de voz, datos e imagen deberá realizar las acciones señaladas en la presente directiva en el tiempo y forma que se señala.

Ing. Enrique Quinto Ceballos Aradillas
Director del Centro de Control, Comando y Comunicación C4
AUTORIZÓ

Lic. Osvaldo Alejandro Hernández León
Director de la red, voz, datos e imagen del Centro de Control, Comando Y Comunicación
REVISÓ

SECRETARÍA DE SEGURIDAD PÚBLICA DEL ESTADO DE OAXACA
CENTRO DE CONTROL, COMANDO Y COMUNICACIÓN C4

Capítulo	6. Operaciones	Subcapítulo	6.8 Sistemas de Computadoras
Número de directiva /Referencia CALEA		Fecha de elaboración	Fecha próxima revisión
		Julio 2020	Julio 2020
6.8.3 Manipulación no Autorizada de los Archivos		Revisión:	
		1	
Alcance		Centro de Control, Comando y Comunicación C4	
Autoriza		Ing. Enrique Quinto Ceballos Aradillas Director General del Centro de Control, Comando y Comunicación.	

FUNDAMENTO LEGAL

- Ley General de Archivos publicada en el Diario Oficial de la Federación el 15 de junio de 2018.
- Ley General del Sistema Nacional de Seguridad Pública publicada en el Diario Oficial de la Federación el 02 de enero de 2009 y reformado el 27-05-2019 – Título Séptimo
- Guía Nacional de Cadena de Custodia
- Ley Federal de Transparencia y Acceso a la Información Pública publicada en el Diario Oficial de la Federación el 09 de mayo de 2016

OBJETIVO

Garantizar la integridad de los archivos de información del Centro de Control, Comando y Comunicación mediante la implementación y ejecución de procedimientos de manipulación autorizada archivos digitales.

DESARROLLO DE LA DIRECTIVA

En la operatividad de las diversas áreas del Centro de Control Comando y Comunicación se recopila información de forma continua, el sustento principal de datos se establece mediante las llamadas por parte de la ciudadanía a través del Centro Estatal de Emergencias, sin embargo diversas áreas de C4 también generan información particular del área que puede ser categorizada como:

a) Información pública
b) Información Clasificada
c) Información reservada
d) Información Confidencial

Manipulación Autorizada y no Autorizada de los Archivos Digitales

a) Manipulación autorizada de archivos digitales: Se considera manipulación autorizada o acceso autorizado a todo permiso de manipulación de archivos solicitado y otorgado a un usuario o grupo de usuarios mediante conductos y procedimientos oficiales e institucionales según los reglamentos, normas vigentes y directrices del Centro de Control Comando y Comunicación, que muestren evidencia, concesión y vigencia del acceso y manipulación a los archivos y a la información, para tal motivo, será válido el acceso de los recursos digitales a los que se acceda: sistemas de información, carpetas compartidas, archivos de datos en diversos formatos, documentos electrónicos, correos electrónicos, etc.

Se deberá considerar como un conducto oficial para concesión de accesos los siguientes elementos:

- Mediante giro de oficio
- Mediante giro de tarjeta informativa
- Mediante correo electrónico institucional
- Documento o contrato de las que emane las funciones del usuario y que determine las atribuciones de acceso y manipulación de información.
- Cualquier otro medio oficial que deje evidencia de la fecha de solicitud, el mando que solicita el acceso, y fines del acceso.

El mismo caso aplica para solicitudes de información que deban ser extraíbles de sistemas, carpetas compartidas, de software de video vigilancia, etc. y almacenados en medios ópticos o digitales, para tales casos el acceso a dichos archivos debe ser registrado en una cadena de custodia, que deberá dejar evidencia de todas las personas implicadas en la extracción de la información, almacenamiento de la información, transporte de la información y todos las personas que manipularon dicho archivo hasta su destino final, para cumplir con cabalidad los protocolos que permitan hacer constar la mismidad y autenticidad de los recursos digitales para efectos jurídicos en materia de justicia.

También debe considerarse acceso autorizado a archivos y a la información cuando en facultad de las funciones del puesto que desempeña un usuario le sea autorizado y permitido acceder y/o consultar información competente a su área o áreas que administre.

Un director, subdirector o coordinador puede acceder a toda la información de su área y autorizar el acceso a dicha información a sus subordinados, o compartir la información con otras áreas del Centro de Control Comando y Comunicación, si las solicitudes son de manera oficial y es efectuada la autorización por parte del Director General de C4 Oaxaca.

b) Manipulación no autorizada de archivos digitales: Se considera una manipulación no autorizada o acceso no autorizado cuando un usuario incurra en cualquiera de los siguientes escenarios:

1. Cuando los datos de acceso de un usuario no hayan sido solicitados mediante un conducto institucional por parte del director del área en que se desempeña un usuario.
2. Cuando los datos de acceso hayan concluido su vigencia, se recomienda que los accesos a los sistemas y otros recursos digitales que compartan archivos e información caduquen cada 3 meses como mínimo como medida de seguridad de acceso, para que las contraseñas sean renovadas constantemente.
3. Cuando por cambio de adscripción o por temporalidad de vacaciones o permisos un usuario herede sus credenciales de acceso a otro usuario para desempeñar sus funciones de forma temporal, para evitar tales casos los directores de área deberán notificar de manera oportuna dichos cambios para realizar las altas y bajas pertinentes mediante conductos institucionales para que se generen evidencias de dichos cambios.
4. Cuando un usuario rompa la cadena de custodia según los protocolos, accediendo a información que no deba visualizar.
5. Cuando un usuario acceda a información contenida en archivos y sistemas de información del Centro de Control, Comando y Comunicación desde equipos de cómputo que no pertenezcan a la Secretaría de Seguridad Pública y conectados a la red de C4 Oaxaca sin previa autorización del Director de dicha institución o actividad.

6. Extracción de información de sistemas o de archivos y almacenamiento de ellos en medios digitales o magnéticos, dispositivos de almacenamiento masivo memorias USB, etc., Para uso personal, u otros fines sin previa autorización por parte del director del área y del director general, o que no existan evidencias de la concesión de dichos privilegios de acceso.
7. Cuando un usuario tiene un cambio de adscripción, separación o baja y esto no fue notificado a los administradores de sistemas para su baja correspondiente y dicho usuario continúa teniendo acceso a los sistemas, archivos o correo electrónico.
8. Cuando un usuario malicioso vulnere la seguridad que no siempre radica en los accesos a la información, si no al acceso a dispositivos familiares o comunes, o mediante software malicioso, de ahí la importancia de que los archivos del Centro de Control Comando y Comunicación solo sea accedida mediante dispositivos de la SSPO.
9. Cuando una información sea clasificada o confidencial, o tenga vigencia de reserva por un periodo determinado y dicha información sea compartida, para tal caso la responsabilidad recaerá en quien comparte dicha información según las evidencias de los conductos institucionales o cadenas de custodia.
10. Cuando se tenga acceso a áreas no autorizadas o de acceso restringido y se manejen temas o se resguarden documentos e información sensible.

Para tales casos se deberán aplicar sanciones según lo considere la Dirección General del Centro de Control Comando y Comunicación y la Dirección, los casos deberán aplicar lo que indiquen las normas y reglamentos internos del Centro de Control Comando y Comunicación, leyes en materia de Seguridad Pública del Estado de Oaxaca, Constitución Política de los Estados Unidos Mexicanos; En caso de que el usuario pertenezca a una corporación de seguridad pública se debe notificar y canalizar el caso para que la corporación aplique correctivos disciplinares y dependiendo de la gravedad de la falta intervenga la Dirección General de Asuntos Internos o autoridades competentes en la materia.

Política para la introducción, remover, alterar, o Descargar archivos o programas de computadora.

Para todos los casos, los usuarios que ejecuten las operaciones de introducción, remoción, alteración o descarga de documentos digitales o programas de computadoras deberán estar facultados en sus funciones como parte las actividades y operaciones de su puesto o contar con autorización por escrito mediante oficio o tarjeta informativa parte de su superior inmediato, quien deberá tener facultad de otorgar dichos permisos de operación a sus subordinados, o en su caso escalar la solicitud a la Dirección General del Centro de Control Comando y Comunicación para que se otorguen a los usuarios dichas facultades de operaciones en archivos digitales o software's de computadora.

A continuación se describen las políticas que los usuarios facultados pueden ejecutar en archivos digitales y software de computadora en el Centro de Control, Comando y Comunicación.

a) **Introducción de archivos y programas digitales de computadora:** Todos los archivos y programas que se generen en cada departamento, por descarga de documentos digitales de diversas fuentes de internet, correo electrónico institucional, por exportación de datos de sistemas de información o sistemas de bases de datos, por captura en software de ofimática para procedimientos de los procesos de rutina de cada puesto en cada una de las áreas, todos los archivos electrónicos generados para fines de los procesos y procedimientos del Centro de Control Comando y Comunicación y la Secretaría de Seguridad Pública de Oaxaca, que se generen o introduzcan a los

procesos desde equipos de cómputo que pertenecen a la institución, se convierten en documentación electrónica que pertenece al área donde fue generada o introducida y requiere un tratamiento apegado a procedimientos que garanticen el correcto acceso y tratamiento de dichos archivos, debido a que la información institucional contenida en dichos documentos electrónicos son un acervo de la Secretaría de Seguridad Pública y por lo tanto del Gobierno del Estado de Oaxaca.

A continuación se describen algunas políticas y consideraciones para la introducción de archivos digitales.

- Los usuarios que creen o introduzcan nuevos archivos digitales o software, deben ser usuarios autorizados con la facultad de crear, introducir y manipular documentos digitales.
- La autorización de dichas operaciones deberá estar definida en la descripción del puesto del usuario, en algún oficio o tarjeta informativa, donde su superior inmediato solicite la concesión de dicha facultad para un usuario o grupo de usuarios, informando de manera oficial de las operaciones que se estén realizando.
- La alta Dirección deberá notificar mediante oficio o tarjeta informativa la autorización de la introducción de archivos digitales o el conocimiento de las operaciones.
- Cuando la introducción de archivos sea una actividad de rutina para el usuario, se recomienda que se agregue como parte de la descripción de las actividades del puesto que ocupa.
- Se recomienda que en los equipos de cómputo de la Secretaría de Seguridad Pública no se introduzcan archivos personales de los usuarios o empleados.
- Cuando un usuario introduzca documentos digitales de fuentes de información contenidos en memorias flash o USB, discos duros externos, etc. Es importante que dichos dispositivos se sometan a un proceso de descontaminación en un equipo destinado a esa labor, que se encuentre debidamente actualizado y comunicar al jefe del área sobre la operación.
- En caso de no contar con un equipo destinado para la descontaminación de dispositivos de almacenamiento masivos externos, canalizar al área de Soporte Técnico y Desarrollo Tecnológico para ejecutar un escaneo y descartar la introducción de Software malicioso a los equipos del Centro de Control, Comando y Comunicación.
- Todo dispositivo de almacenamiento masivo externo que se utilice para introducir o compartir archivos a los equipos de cómputo del Centro de Control, Comando y Comunicación deben pertenecer a la Secretaría de Seguridad Pública, y se debe informar mediante un documento institucional al jefe del área de los archivos digitales que se están manejando desde unidades o memorias flash.
- Si el jefe de área lo considera necesario pueden implementar cadenas de custodia de archivos digitales, con la finalidad de llevar un control más estricto de la manipulación de los archivos, con una bitácora que describa quién introduce el archivo o quién crea el archivo, quién o quienes modifican el archivo, quién borra el archivo, o quién difunde el archivo con las observaciones donde escriba los motivos, con fechas y horas. Este tipo de acciones son recomendables para implementar sobre todo cuando se manipulen archivos digitales que contienen información altamente sensible, confidencial, de carácter que requiera ser catalogado como no público.
- En caso de que sea sumamente necesaria la manipulación de archivos digitales desde unidades flash y que esta sean unidades personales, el jefe de área deberá estar enterado

y autorizar dichas operaciones e implementar medidas se seguridad, como bitácoras o cadenas de custodia en caso de ser necesario.

- Para el caso de la introducción o descarga de programas o sistemas de información, todo el software utilizado en el Centro de Control Comando y Comunicación debe ser propiedad de la institución, desarrollado por la institución o adquirido por compra de licencias, o como renta de un servicio o póliza de servicio para la utilización de software o en su caso software de licenciamiento libre.
- Todo software introducido o descargado por parte de un usuario final, debe ser informado y autorizado por el jefe inmediato superior o jefe del área mediante conductos institucionales, en caso de no tener el perfil para la correcta valoración del software, se puede dirigir a las áreas especializadas con la finalidad de asegurar el cumplimiento de las directivas.
- Todo software introducido o descargado de internet, que no cumpla con las dos condiciones anteriores será responsabilidad del usuario del equipo de cómputo, para lo cual el jefe del área o la alta dirección podrán indicar las sanciones correspondientes o dependiendo del de la gravedad del caso escalar o canalizarlo a la Dirección General de Asuntos Internos.

Cuando un usuario infringe con las políticas anteriormente mencionadas, se deberá considerar su operación de introducción de archivos digitales o programas de computadoras como una operación NO autorizada, por lo que el caso podrá ser reportado por el superior inmediato a la alta Dirección del Centro de Control, Comando y Comunicación para la ejecución de sanciones.

b) Remover archivos o software de computadora: Se refiere al borrado de archivos digitales o al borrado de programas contenidos en equipos de cómputo del Centro de Control, Comando y Comunicación de Estado de Oaxaca.

A continuación se describen algunas políticas y consideraciones para el borrado de archivos digitales o software de computadora:

- Los usuarios que borren archivos digitales o software de computadora, deben ser usuarios autorizados con la facultad de remover documentos digitales o programas de computadoras.
- La autorización de dichas operaciones deberá estar definidas en la descripción del puesto del usuario o en algún oficio o tarjeta informativa, donde su superior inmediato solicite la concesión de dicha facultad para un usuario o grupo de usuarios, o por lo menos informe de manera oficial de las operaciones que se están ejecutando.
- La alta Dirección deberá notificar mediante oficio o tarjeta informativa la autorización de la introducción de archivos digitales o el conocimiento de las operaciones.
- Cuando la remoción de archivos sea una actividad de rutina para el usuario, se recomienda que se agregue como parte de la descripción de las actividades del puesto que ocupa.
- Antes de ejecutar cualquier procedimiento de eliminación de archivos o de software, el proceso debe ser informado por el usuario a sus superiores inmediatos, cuando el proceso sea parte de las actividades de rutina, se debe establecer un documento oficial en el que se indique el procedimiento, la periodicidad, y la descripción de la actividad.
- En caso de no ser una actividad de rutina por cada vez que se ejecute un proceso de borrado de archivos o software se debe informar al jefe del área de dicho proceso antes de ser ejecutado.

- Sin una instrucción oficial, usuario final no está autorizado ni facultado para borrar archivos que contengan información del Centro de Control, Comando y Comunicación y sus diversas áreas, de la Secretaría de Seguridad Pública de Oaxaca o del Gobierno del Estado de Oaxaca a menos que su superior inmediato lo instruya, por lo cual deberá dejar un precedente en donde documente en un oficio el motivo del borrado del o de los archivos, o de la desinstalación o borrado del software del equipo de cómputo.
- Todo usuario que borre archivos, desinstale o borre software del Centro de Control, Comando y Comunicación del Estado de Oaxaca sin previa autorización o sin ser parte de sus funciones, será reportado por su superior inmediato a la Dirección General del Centro de Control, Comando y Comunicación de Oaxaca por medio de un oficio o tarjeta informativa, y canalizado para que la alta Dirección aplique una sanción acorde a la gravedad del caso.

Cuando un usuario incumpla con las políticas mencionadas anteriormente, se deberá considerar su operación de remoción de archivos digitales o programas de computadoras como una operación NO autorizada, por lo que podrá ser reportado por su superior inmediato a la alta Dirección del Centro de Control, Comando y Comunicación para ejecutar sanciones.

c) Alterar archivos o Software de Computadora: La alteración de estos documentos digitales debe ser realizada por personal autorizado acorde a sus funciones o sus instrucciones. A continuación se describen algunas políticas y consideraciones para la alteración de archivos digitales o software de computadora:

- Los usuarios que alteren archivos digitales o software de computadora, deben ser usuarios autorizados con la facultad de alterar documentos digitales o programas de computadoras.
- La autorización de dichas operaciones deberá estar definidas en la descripción del puesto del usuario o en algún oficio o tarjeta informativa, donde su superior inmediato solicite la concesión de dicha facultad para un usuario o grupo de usuarios, o por lo menos informe de manera oficial de las operaciones que se están ejecutando.
- La alta Dirección deberá notificar mediante oficio o tarjeta informativa la autorización de la introducción de archivos digitales o el conocimiento de las operaciones.
- Cuando la remoción de archivos sea una actividad de rutina para el usuario, se recomienda que se agregue como parte de la descripción de las actividades del puesto que ocupa.
- El proceso de alteración de archivos o programas de computadora debe ser parte de las funciones del usuario debidamente autorizado que lo ejecuta en la institución, o por instrucción directa de su superior inmediato o jefe del área.
- Cuando la alteración de documentos digitales o software involucre información sensible, confidencial o imprescindible para el área o la institución es necesaria la elaboración de un documento oficial para marcar la evidencia de la manipulación y alteración de dichos archivos o software.
- Toda alteración de archivos digitales o software de computadora debe ser dentro del marco de legalidad estipulados en los reglamentos institucionales y las leyes federales y Estatales vigentes.

Cuando un usuario infrinja las políticas anteriormente mencionadas, se deberá considerar su operación de alteración de archivos digitales o programas de computadoras como una operación NO autorizada, por lo que su superior inmediato reportará el caso a la alta Dirección del Centro de Control, Comando y Comunicación para la ejecución sanciones.

d) **Bajar archivos o programas de computadora:** Se refiere a la descarga de archivos digitales o software de la red o internet en los equipos del Centro de Control Comando y Comunicación. A continuación se describen algunas políticas y consideraciones para la alteración de archivos digitales o software de computadora:

- Los usuarios que descarguen archivos digitales o software de computadora, deben ser usuarios autorizados con la facultad de descargar documentos digitales o programas de computadoras.
- La autorización de dichas operaciones deberá estar definidas en la descripción del puesto del usuario o en algún oficio o tarjeta informativa, donde su superior inmediato solicite u otorgue la concesión de dicha facultad para un usuario o grupo de usuarios, o por lo menos informe de manera oficial de las operaciones que se están ejecutando.
- La alta Dirección deberá notificar mediante oficio o tarjeta informativa la autorización de las descargas de archivos digitales o el conocimiento de las operaciones.
- Cuando las descargas de archivos seas una actividad de rutina para el usuario, se recomienda que se agregue como parte de la descripción de las actividades del puesto que ocupa.
- Tal y como se menciona en el apartado de "introducción de software de computadora", todo software descargado de internet y que se instale en los equipos de cómputo del Centro de Control, Comando y Comunicación debe ser solicitado y autorizado al jefe del área o superior inmediato para justificar su descarga e instalación, bajo el entendido de que dicho software debe contar con un licenciamiento libre. En caso de ser necesario se podría canalizar dicha solicitud a la Coordinación de Soporte Técnico y Desarrollo Tecnológico, quienes determinarán el tipo de licencia de software o alguna alternativa de solución para el requerimiento.
- Se recomienda que los equipos que descargan constantemente archivos o software de internet cuenten con la instalación antivirus activado con licencia y actualizado que se encuentre continuamente actualizado.
- La descarga de archivos digitales o software ilegales, sin previo informe y autorización será responsabilidad del usuario final lo que puede tener sanciones establecidas y definidas por la alta dirección y hasta repercusiones legales.

Cuando un usuario no cumpla con las políticas anteriormente descritas, se deberá considerar su operación de descarga de archivos digitales o programas de computadoras como una operación NO autorizada, por lo que su superior inmediato reportará el caso a la alta Dirección del Centro de Control, Comando y Comunicación para ejecutar sanciones.

RESPONSABLES

- El Director General del Centro de Control, Comando y Comunicación: Encargado de verificar que se apliquen las recomendaciones de la presente directiva por parte del personal a su cargo.
- El Director del Centro Estatal de Emergencias: Encargado de verificar que se apliquen las recomendaciones de la presente directiva por parte del personal a su cargo.
- El Director de la red de Voz, Datos e Imagen: Encargado de verificar que se apliquen las recomendaciones de la presente directiva por parte del personal a su cargo.
- Todas las coordinaciones de las diversas áreas del Centro de Control, comando y Comunicación: Quienes se tienen que apegar a las recomendaciones de la presente directiva.
- Todos los usuarios de las coordinaciones de las diversas áreas del C4: Quienes se tienen que apegar a las sugerencias de la presente directiva.

Ing. Enrique Quinto Ceballos Aradillas
Director del Centro de Control, Comando y Comunicación C4
AUTORIZÓ

Lic. Osvaldo Alejandro Hernández León
Director de la red, voz, datos e imagen del Centro de Control, Comando Y Comunicación
REVISÓ

SECRETARÍA DE SEGURIDAD PÚBLICA DEL ESTADO DE OAXACA
CENTRO DE CONTROL, COMANDO Y COMUNICACIÓN C4

Capítulo	6. Operaciones	Subcapítulo	6.8 Sistemas de Computadoras
Número de directiva /Referencia CALEA		Fecha de elaboración	Fecha próxima revisión
		Septiembre 2020	Septiembre 2020
6.8.4 Uso de computadoras, políticas y procedimientos		Revisión:	
		2	
Alcance		Centro de Control, Comando y Comunicación C4	
Autoriza		Ing. Enrique Quinto Ceballos Aradillas Director General del Centro de Control, Comando y Comunicación.	

FUNDAMENTO LEGAL

- Constitución Política de los Estados Unidos Mexicanos
- Ley General de Transparencia y Acceso a la Información Pública
- Ley federal de Transparencia y Acceso a la Información Pública
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Ley de Protección de Datos Personales en Posesión de Sujetos obligados del Estado de Oaxaca.
- Ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca.
- Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia.
- lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.
- Lineamientos que deberán observar los sujetos obligados para la atención de requerimientos, observaciones, recomendaciones y criterios que emita el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
- Documentos técnicos, metodológicos y normativos de la fracción XXX del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.

OBJETIVO

Establecer políticas mediante la normatividad del acceso y uso de sistemas, seguridad de servidores, estaciones de trabajo, sistemas portátiles, equipos de cómputo y dispositivos móviles alámbricos e inalámbricos para que el uso de los equipos sea apropiado y destinado para fines institucionales.

DESARROLLO DE LA DIRECTIVA

En el Centro de Control, Comando y Comunicación del Estado de Oaxaca se desarrollan actividades que constantemente requieren de la implementación de Tecnologías de la Información y Comunicaciones, que comprende: equipos de cómputo, tecnología celular, radios, sistemas de información, correo electrónico, acceso a internet, acceso a redes sociales etc. La presente directiva establece que todos los recursos tecnológicos, ya sean alámbricos e inalámbricos, que se encuentren en las instalaciones de C4 Oaxaca, deben ser estrictamente orientados y usados para el desempeño de las funciones de los trabajadores de las diversas áreas para el desarrollo de actividades exclusivamente para fines institucionales.

Para efectos de la presente directiva se definen los siguientes conceptos:

Equipo de Cómputo: Todos los Equipos Electrónicos y Dispositivos de Comunicación que pertenecen al Centro de Control, Comando y Comunicación: Computadoras, CPU, Monitores, Teclados, Mouses, Servidores, RACK, Drivers, Escáner, Plotters, Dispositivos móviles, etc.

Internet: es la conexión vía cable o inalámbrica con la que las computadoras cuentan dentro de la red de las instalaciones de C4 Oaxaca, para conectarse y visualizar páginas web y sistemas de información desde un navegador y acceder a otros servicios que ofrece esta red.

Correo Electrónico: Buzón de correspondencia electrónica generado y administrado por El Área de Sistemas de C4 Oaxaca.

a) Responsabilidad y riesgos que involucran

- El equipo de Cómputo, deberá utilizarse como herramienta de apoyo y está limitado a labores específicamente relacionadas con funciones asignadas al cargo de cada trabajador. El uso del equipo de cómputo contempla el empleo del hardware y software que se encuentre instalado en las mismas, incluyendo el acceso a Internet, cuando se disponga de conexión a la red y sistemas de información.
- Es responsabilidad del usuario, hacer buen uso del equipo de cómputo asignado, así como la conservación, integridad y contenidos de la información que se encuentra en los discos duros de los equipos de escritorio y portátiles.
- El acceso y uso de las Tecnologías Informáticas y de Comunicación se debe entender como un privilegio que otorga el Centro de Control, Comando y Comunicación a sus empleados, no como un derecho. Por lo anterior, el acceso y uso a estos recursos informáticos conlleva la responsabilidad de cumplir estrictamente las políticas descritas en el presente documento.
- Es responsabilidad del área administrativa del Centro de Control, Comando y Comunicación hacer de conocimiento mediante la lectura y firma de enterado de las directivas y reglamentos internos vigentes a todos los empleados de nueva contratación y ya contratados.
- Es responsabilidad de los usuarios reportar mediante tarjeta informativa a su superior inmediato cuando algún componente de sus equipos de cómputo comience a fallar, cuando requiera la instalación de algún nuevo software, o cambiar su nivel de acceso a sistemas según lo requiera para el desempeño de sus funciones laborales.
- Es responsabilidad de los supervisores o coordinadores de área notificar mediante tarjeta informativa a su director de área, y a su vez solicitar a la Dirección de Red, Voz, Datos e Imagen la solicitud para la revisión, mantenimiento, valoración para reemplazo de equipo o pieza, cambio de software, cambio de nivel de acceso a internet o sistemas de información.
- Es responsabilidad de la Dirección de Red, Voz, Datos e Imagen notificar mediante tarjeta informativa, la atención que se le dio a uno o varios equipos y si se requiere de algún cambio para que el área correspondiente proceda a la solicitud al área de almacén.
- Es responsabilidad del jefe de área, supervisor o coordinador vigilar que las políticas de la presente directiva se cumplan, orientar a sus subordinados, y en caso de incumplimiento reportar mediante tarjera informativa a su Director inmediato para que se apliquen los correctivos disciplinares correspondientes.
- El no cumplimiento de las Políticas descritas en la presente directiva se entenderá como una falta grave al reglamento interno de trabajo, lo cual puede llevar a sanciones disciplinarias incluyendo: llamadas de atención, levantamiento de actas administrativas, indemnizaciones o reposición de los equipos dañados, hasta la terminación del contrato laboral del empleado.

b) Riesgos a las computadoras y a los programas de software;

Existen dos perspectivas de los riesgos de computadoras, el aspecto físico y el aspecto lógico. Ambos se contemplan para evitar daños potenciales a los equipos.

- Es obligatorio cancelar el consumo de bebidas y alimentos cerca de los equipos de cómputo porque existe un riesgo que se derrame o manchen los equipos, lo que puede ocasionar fallos temporales o permanentes.
- El polvo es un factor de riesgo de fallos en los equipos, por lo que es responsabilidad del empleado mantener limpio y libre de polvo su área de trabajo y los equipos de cómputo que utiliza.
- Es un riesgo para las computadoras la instalación de software pirata que generalmente usa crack's o parches que permiten la utilización de software de licenciamiento de pago.
- También se considera un riesgo descargar archivos de internet de desarrolladores desconocidos o sin licenciamiento apropiado.
- Los dos puntos anteriores son factores de riesgo porque ese tipo de procedimientos instala software que deja al equipo de cómputo con vulnerabilidades de: virus, malware, pishing, ataques informáticos, sabotajes, exposición de información sensible, gusanos informáticos. Etc.

c) Expectativas de privacidad

Todos los equipos de cómputo y recursos de Tecnologías de la información del Centro de Control, Comando y Comunicación pertenecen a la Secretaría de Seguridad Pública de Oaxaca y al Gobierno del Estado de Oaxaca. Por tal motivo toda la información y archivos digitales que se guarden o comparten mediante estos dispositivos se convierten en un recurso público del Estado, que estarán normados por la Ley de Protección de Datos Personales en Posesión de Sujetos obligados del Estado de Oaxaca y por la Ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca.

Con esta premisa se debe considerar que en los equipos de cómputo del Centro de Control, Comando y Comunicación no existirá privacidad para los usuarios, debido a que los equipos de cómputo son recursos públicos, los usuarios no se deben guardar archivos personales, ni información personal en los equipos, ya que dichos datos podrían ser accedidos y consultados por otros usuarios de su mismo puesto o de rango superior de su misma área.

d) Actividades autorizadas

Se considera actividades autorizadas todas aquellas que involucren e impliquen el desarrollo de las funciones descritas en el puesto que desempeñe el empleado, descrito según el manual de la organización o la ejecución de funciones instruidas por su superior inmediato. Todas estas actividades deben ser de carácter o con fines institucionales y pueden involucrar la operación de equipos de cómputo, sistemas de información, acceso a internet, dispositivos móviles, correo electrónico institucional, etc. De forma general se pueden mencionas las siguientes:

- Consulta, envío y recepción de correo electrónico institucional
- Navegación en internet, según el nivel de acceso que solicite un jefe de área para sus subordinados o para cada usuario en particular.
- Accesos a sistemas de información según su perfil en la institución.
- Utilización de equipo de cómputo e impresoras para fines institucionales
- El uso de la red inalámbrica es exclusivo para el personal autorizado, se habilitará el servicio previa solicitud vía tarjeta informativa, con justificación y autorización del responsable de área correspondiente.

e) Actividades prohibidas

Se consideran actividades prohibidas todas aquellas actividades que orientan los recursos tecnológicos de la institución para uso personal y que no benefician ni apoyan a las tareas institucionales. Entre las actividades no autorizadas que por lo tanto están prohibidas podemos mencionar las siguientes:

- Utilizar los equipos de Cómputo y Espacios Compartidos, para el almacenamiento de información y archivos personales.
- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.
- Acceder sin la debida autorización, mediante computadores, software, información o redes de la Institución, a recursos externos o que pertenezcan al Centro de Control, Comando y Comunicación.
- Interferir sin autorización el acceso a otros usuarios a los recursos de los sistemas de información.
- Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
- Utilizar los sistemas de información para propósitos ilegales o no autorizados.
- Enviar cualquier comunicación electrónica fraudulenta.
- Violar cualquier licencia de software o derechos de autor, incluyendo la copia o distribución de software protegido legalmente sin la autorización escrita del propietario del software.
- Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.
- Usar las comunicaciones electrónicas para acosar o amenazar a los usuarios de la Institución o externos, de alguna manera que sin razón interfiera con la educación o el desempeño de los empleados.
- Usar las comunicaciones electrónicas para revelar información privada sin el permiso explícito del propietario o responsable.
- Leer o visualizar la información o archivos de otros usuarios sin su permiso.
- Cualquier tipo de deshonestidad laboral.
- Alterar, falsificar o de alguna otra forma usar de manera fraudulenta la información de la Institución o cualquiera externo (incluyendo información computarizada, permisos, documentos electrónicos, u otros documentos o propiedades digitales).
- Usar las comunicaciones electrónicas para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente: esto incluye la descarga no autorizada de archivos y programas de internet.
- Lanzar cualquier tipo de virus, gusano, o programa de computador cuya intención sea hostil o destructiva.
- Uso personal de cualquier sistema de información de la Institución para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material obsceno.
- Violar cualquier ley o regulación nacional respecto al uso de sistemas de información.
- Acceder a sitios de internet que no contribuyan al desarrollo de las actividades institucionales, como redes sociales, sitios de mensajería instantánea, sitios pornográficos. Etc.
- La descarga de material de ocio, como archivos de audio y video en diversos formatos.
- Escuchar la radio y ver televisión por Internet. Salvo en aquellos casos que se justifique, contando con el visto bueno del responsable de área correspondiente.
- Queda estrictamente prohibido la instalación y utilización de software de que haga uso indiscriminado del ancho de banda de la red, por ejemplo: Kazaa, Ares, Gator, Audio Galaxy, YouTube, y aplicaciones P2P, ver televisión o escuchar la radio haciendo mal uso del enlace a Internet.

f) Revisión administrativa de las actividades

- Las consultas a internet estarán monitoreadas constantemente con hardware y software de red especializado, el área de sistemas reportará anomalías de seguridad mediante tarjeta informativa cada año a las diversas direcciones que se encuentran físicamente en C4 Oaxaca, según se requiera.
- El área de sistemas ejecutará revisiones programadas con las diversas Direcciones, que pueden coincidir con las temporadas de mantenimiento (cada año) de los equipos, en los cuales se verificará que todo el software y sistemas que contienen los equipos tengan licenciamiento adecuado, que no exista software pirata, software malicioso. Y en caso de encontrar casos, se deberá reportar a la Dirección de Red, Voz, Datos e Imagen para que informe a la Dirección a la que se aplica la revisión mediante Oficio la información que corresponda.
- Es responsabilidad del área administrativa del Centro de Control, Comando y Comunicación hacer de conocimiento mediante la lectura y firma de enterado de las directivas y reglamentos internos vigentes a todos los empleados de nueva contratación y ya contratados.

RESPONSABLES

El Director General del Centro de Control, Comando y Comunicación: Aplica sanciones correspondientes; Podrá recibir copia o reportes directos de reportes de uso inadecuado de correo electrónico, internet o computadoras.

El Director del Centro Estatal de Emergencias Podrá recibir copia o reportes directos de reportes de uso inadecuado de correo electrónico, internet o computadoras. Aplica sanciones correspondientes, cuando son casos muy graves, reporta al Director general mediante tarjeta informativa.

El Director de la red de Voz, Datos e Imagen: Podrá recibir copia o reportes directos de reportes de uso inadecuado de correo electrónico, internet o computadoras. Aplica sanciones correspondientes, cuando son casos muy graves, reporta al Director general mediante tarjeta informativa.

Todas las coordinaciones de las diversas áreas del Centro de Control, comando y Comunicación: Quienes se tienen que apegar a las recomendaciones de la presente directiva: Son los que verifican que sus subordinados cumplan con lo estipulado en la presente directiva, reporta a su superior inmediato en caso de que un subordinado no la cumpla para que se apliquen sanciones correspondientes.

Coordinador de Soporte Técnico y Desarrollo Tecnológico: Instruye para que se ejecuten revisiones periódicas de equipos de cómputo, o de lo que se consulta en internet en caso que lo soliciten los Directores.

Usuarios: quienes se apegarán a los lineamientos estipulados en la presente directiva.

Ing. Enrique Quinto Ceballos Aradillas
Director del Centro de Control, Comando y Comunicación C4
AUTORIZÓ

Lic. Osvaldo Alejandro Hernández León
Director de la red, voz, datos e imagen del Centro de Control, Comando Y Comunicación
REVISÓ

SECRETARÍA DE SEGURIDAD PÚBLICA DEL ESTADO DE OAXACA
CENTRO DE CONTROL, COMANDO Y COMUNICACIÓN C4

Capítulo	6. Operaciones	Subcapítulo	6.8 Sistemas de Computadoras
Número de directiva /Referencia CALEA		Fecha de elaboración	Fecha próxima revisión
		Noviembre 2020	Noviembre 2020
6.8.5 Sistema de Seguridad		Revisión:	
		1	
Alcance		Centro de Control, Comando y Comunicación C4	
Autoriza		**Ing. Enrique Quinto Ceballos Aradillas** Director General del Centro de Control, Comando y Comunicación.	

FUNDAMENTO LEGAL

- ISO 27001
- ISO 27001:2013
- ISO 27002.

OBJETIVO

Realizar una inspección documentada cada tres meses, de los archivos y de los sistemas de seguridad en las computadoras, con la finalidad de identificar violaciones a las políticas de uso de equipos de cómputo o el uso inadecuado de los sistemas de información.

DESARROLLO DE LA DIRECTIVA

La inspección de los archivos y de los sistemas de seguridad, como claves de acceso o contraseñas a los equipos de cómputo asignados al Centro de Control, Comando y Comunicación, se realizará cada tres meses, como se describe a continuación:

Primera inspección	Segunda inspección	Tercera inspección	Cuarta inspección
Marzo	Junio	Septiembre	Diciembre

El Área de soporte técnico y Desarrollo Tecnológico tiene la responsabilidad de inspeccionar cada 3 meses los equipos de cómputo, para determinar que los accesos por medio de las contraseñas hayan sido correctos por el usuario, de acuerdo a los permisos o roles asignados a la contraseña.

Revisando el nivel de seguridad instalada por los antivirus, que éstos cuenten con las últimas actualizaciones de las bases de datos de virus, verificando que la última fecha del escaneo en busca de virus y programas maliciosos sea recientes para estar seguro que los equipos están limpios de cualquier amenaza que puedan poner en riesgo la integridad física de la información.

Durante la inspección se verifica que el usuario no tenga instalado ningún otro tipo de software que pueda poner en riesgo la integridad del equipo tanto en hardware como software, o que en su caso tenga responsabilidades con los derechos de autor.

En caso de detectar que los sistemas de seguridad como antivirus, firewalls, estén vencidos o desactualizados, instalar inmediatamente una licencia nueva actualizada que cumpla con las normas de derecho de autor.

La actividad de inspección realizada cada tres meses quedará registrada en la bitácora digital correspondiente:

RESPONSABLES

- Personal de la Coordinación de Soporte Técnico y Desarrollo Tecnológico: Quienes en cada periodo ejecutan una revisión y registran de forma digital todas las observaciones realizadas en cada inspección.

- Los usuarios finales: quienes acatan las recomendaciones de seguridad que les la el personal de Soporte Técnico y Desarrollo Tecnológico tras la inspección.

Ing. Enrique Quinto Ceballos Aradillas
Director del Centro de Control, Comando y Comunicación C4
AUTORIZÓ

Lic. Osvaldo Alejandro Hernández León
Director de la red, voz, datos e imagen del Centro de Control, Comando Y Comunicación
REVISÓ

Capítulo	6. Operaciones	Subcapítulo	6.8 Sistemas de Computadoras
Número de directiva /Referencia CALEA		Fecha de elaboración	Fecha próxima revisión
		Noviembre 2020	Noviembre 2020
6.8.6 Respaldo de Computadoras		Revisión:	
		2	
Alcance		Centro de Control, Comando y Comunicación C4	
Autoriza		Ing. Enrique Quinto Ceballos Aradillas Director General del Centro de Control, Comando y Comunicación.	

FUNDAMENTO LEGAL

Ley General de Archivos publicada en el Diario Oficial de la Federación el 15 de junio de 2018.

Ley General del Sistema Nacional de Seguridad Pública publicada en el Diario Oficial de la Federación el 02 de enero de 2009 y reformado el 27-05-2019 – Título Séptimo

Guía Nacional de Cadena de Custodia

Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.- Consejo Nacional.- CONAIP/SNT/ACUERDO/EXT13/04/2016-03

Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video vigilancia para la seguridad pública. Instituto Politécnico Nacional (Octubre de 2016)

Norma técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video-vigilancia para la seguridad pública. Anexo Técnico. (Centro Nacional de Información, SEGOB, y Secretariado Ejecutivo del sistema nacional de Seguridad Pública.

OBJETIVO

Establecer buenas prácticas en los procesos de respaldo de información computarizada y el asentamiento de bases para generar evidencia que facilite la comprobación de la ejecución exitosa de dichos procesos con la finalidad de garantizar la calidad de los respaldos de información que se realizan en el Centro de Control Comando y Comunicación del Estado de Oaxaca.

DESARROLLO DE LA DIRECTIVA

El Centro de Control Comando y Comunicación del Estado de Oaxaca en los procesos de sus diversas áreas recopila o genera datos que son procesados mediante Sistemas de Información las cuales son herramientas de gestión de información que se especializan en el tratamiento de datos, captura, almacenamiento, edición, borrado, y procesamiento lógico para la optimización, manipulación y análisis mediante el cual se genera información útil para la toma oportuna de decisiones.

Uno de los grandes retos es la preservación de la información y el aseguramiento para que su conservación histórica sea íntegra, persistente y consistente, como medida de protección ante el caso de alguna contingencia que involucre alguna pérdida de información total o parcial.

En la presente directiva se establecen algunos criterios para el aseguramiento de la calidad de los procesos de respaldo de información computarizada, contemplando los siguientes aspectos:

a) Respaldo, uso y almacenamiento de los archivos computarizados.

Un respaldo de información es la ejecución de una copia de seguridad de datos, información, archivos, documentos digitales, etc. Como medida de prevención de pérdida de datos ante cualquier eventualidad o desastre que ponga en peligro la integridad de la información o la operatividad de una organización.

Los respaldos son utilizados en las organizaciones como una medida de protección ante cualquier siniestro natural o fallos del sistema de hardware que impliquen corrupción de datos o pérdida parcial o total de información la cual es el recurso más valioso de una institución, ya que es el resultado de las operaciones de sus procesos o es lo que permite seguir sus operaciones.

Cuando se ejecuta un respaldo de información generalmente se hace un copiado total o parcial de los datos en un medio de almacenamiento, que podría ser local, remota, externa o en línea, siempre es recomendable que un respaldo se ejecute almacenando los datos copiados en un medio que no sea la fuente principal de la información, con la premisa de que si esta llega a fallar, el respaldo no sufra pérdidas de datos o daño.

Un respaldo es como un seguro de la información que se tiene que establecer a la medida y acorde a las necesidades y prioridades de la organización. Los respaldos de computadoras en el Centro de Control, Comando y Comunicación de Oaxaca pueden realizarse en varios ámbitos, de los principales podemos citar los siguientes:

- **Respaldos de bases de datos:** Los sistemas gestores de bases de datos que podrían ser relacionales (Los que no manejan lenguaje SQL) y no relacionales (Los que no manejan SQL) son programas que son encargados de garantizar la integridad de la información, ofreciendo una alta gama de ventajas muy superior comparada con el manejo de información en archivos. Dichos sistemas ofrecen características como el acceso concurrente por parte de múltiples usuarios, la integridad de los datos, accesibilidad, independencia lógica y física de los datos, redundancia mínima, consultas complejas optimizadas, seguridad de acceso y auditoría, acceso a través de lenguajes de programación estándar, respaldo y recuperación.

  Es recomendable que toda la información sensible y vital para la organización sea almacenada en bases de datos y gestionada mediante sistemas de información, las bases de datos ofrecen la gran ventaja del manejo de respaldos que se pueden programar de acuerdo a las necesidades de la institución. Con esto se podrá garantizar la restauración de los datos en caso de contingencias o desastres que conlleven a pérdidas de información.

  Procedimientos para la ejecución de respaldos de bases de datos:

  1. Las tareas de respaldo de bases de datos, solo podrán ser ejecutadas por el personal capacitado, autorizado, y que dicha facultad sea parte de sus funciones, en este caso para los Administradores de Infraestructura Tecnológica y los Administradores de Bases de datos.
  2. Como primer paso los administradores de infraestructura y de Bases de datos generarán un informe inicial dirigido al Director de Voz datos, e Imagen mediante tarjeta informativa, dicho informe deberá contener un listado de bases de datos que se manejen en el área, una breve descripción, la cantidad de almacenamiento en disco duro que ocupa, y un estatus donde indique si es información sensible o no. Cuando se implementen nuevas bases de datos, se deberá notificar de la misma forma al director de la Red, Voz, Datos e imagen.
  3. Los usuarios con facultad de ejecutar respaldos de bases de datos determinarán acorde a las capacidades técnicas de la infraestructura y la sensibilidad de la información la periodicidad de

la ejecución de las mejores prácticas y estrategias de respaldos de bases de datos, esto deberá quedar asentado por oficio o tarjeta informativa dirigida al Director de la Red, Voz, Datos e Imagen, si son bases de datos concernientes al Centro Estatal de Emergencias se deberá turnar copia al director del Centro Estatal de Emergencias , y en todos los casos se deberá turnar copia al director General del Centro de Control, Comando y Comunicación.

4. En caso de que las condiciones técnicas cambien, o en caso de alguna modificación en el proceso de respaldo de bases de datos, se deberán notificar mediante oficio o tarjeta informativa al Director de la Red, Voz, Datos e Imagen, si son bases de datos concernientes al Centro Estatal de Emergencias se deberá turnar copia al director del Centro Estatal de Emergencias, y en todos los casos se deberá turnar copia al director General del Centro de Control, Comando y Comunicación.
5. Los administradores de bases de datos o administradores de infraestructura tecnológica deberán llevar una bitácora de respaldos de bases de datos, donde irán registrando los datos del usuario que ejecuta los respaldos en caso de que sean varias personas las que ejecuten la tarea, las fecha y hora de ejecución del respaldo, los datos de la base de datos que se está respaldando, y el medio de almacenamiento destino del respaldo, finalmente; el nombre y cargo del responsable del resguardo del respaldo.
6. Se deberá generar un informe resumido de forma anual mediante oficio o tarjeta informativa dirigida al Director de voz, Datos e Imagen donde se especifiquen las bases de datos respaldadas, la cantidad de respaldos que se ejecutaron, el estatus del almacenamiento de respaldo, el destino o medio de almacenamiento y el nombre del responsable del resguardo de respaldo.
7. Cuando los respaldos no se ejecuten de manera adecuada, los administradores de bases de datos y de infraestructura deberán notificar mediante tarjeta informativa al director de la Red, Voz, Datos e Imagen.
8. Solo el personal técnico: Administradores de Infraestructura Tecnológica y Administradores de Bases de Datos podrán hacer uso y manipulación de los respaldos de bases de datos, debido a que son los que están facultados y capacitados para dichas tareas.
9. Los usuarios con facultad de ejecutar respaldos de bases de datos determinarán acorde a las capacidades técnicas de la infraestructura y la sensibilidad de la información la periodicidad de la ejecución de las mejores prácticas y estrategias de respaldos de bases de datos, esto deberá quedar asentado por oficio o tarjeta informativa dirigida al Director de la Red, Voz, Datos e Imagen, si son bases de datos concernientes al Centro Estatal de Emergencias se deberá turnar copia al director del Centro Estatal de Emergencias , y en todos los casos se deberá turnar copia al director General del Centro de Control, Comando y Comunicación.
10. En caso de que las condiciones técnicas cambien, o en caso de alguna modificación en el proceso de respaldo de bases de datos, se deberán notificar mediante oficio o tarjeta informativa al Director de la Red, Voz, Datos e Imagen, si son bases de datos concernientes al Centro Estatal de Emergencias se deberá turnar copia al director del Centro Estatal de Emergencias, y en todos los casos se deberá turnar copia al director General del Centro de Control, Comando y Comunicación.
11. Los administradores de bases de datos o administradores de infraestructura tecnológica deberán llevar una bitácora de respaldos de bases de datos, donde irán registrando los datos del usuario que ejecuta los respaldos, en caso que sean varias personas las que ejecuten la tarea, las fechas y horas de ejecución del respaldo, la información de la base de datos que se está respaldando, y el medio de almacenamiento destino del respaldo y finalmente haciendo mención del responsable del resguardo del respaldo.

12. Se deberá generar un informe resumido de forma anual mediante oficio o tarjeta informativa dirigida al Director de voz, Datos e Imagen donde se especifiquen las bases de datos respaldadas, la cantidad de respaldos que se ejecutaron, el destino o medio de almacenamiento del responsable del resguardo de respaldo.

- **Respaldos de código fuente de sistemas de información:** Los sistemas de información cuando deben ser respaldados para poder ser restaurados en caso de fallos de servidores, la estrategia más óptima es la implementación de un sistema de control de versiones que almacene todas las versiones y cambios o actualizaciones de los módulos de los sistemas, dicha implementación puede programarse con una arquitectura que permita el almacenamiento de los cambios en una fuente principal y otra secundaria la cual se recomienda no resida en el mismo servidor, estas fuentes deben ser independientes de la rama de producción.

  Procedimientos para la ejecución de respaldos de código fuente de sistemas de información:

  1. La coordinación de Soporte Técnico y Desarrollo Tecnológico deberá informar de manera anual mediante tarjeta informativa a la Dirección de Red, Voz, Datos e Imagen un listado de sistemas de software que se han desarrollado en el área, dicho informe deberá contener el nombre de cada sistema, una breve descripción y su estatus que pueden ser las siguientes opciones: en producción, en pruebas, en desarrollo, inhabilitado o en mantenimiento. En el contenido del informe se deberá especificar la fuente de almacenamiento de los respaldos del código fuente y el responsable del resguardo de dichos respaldos.
  2. Las tareas de respaldo de código fuente de sistemas de información desarrolladas en el Centro de Control, Comando y Comunicación, involucran a los desarrolladores de sistemas del área del Soporte Técnico y Desarrollo Tecnológico, quienes deberán registrar los cambios que van haciendo a los sistemas de información en un sistema de control de versiones de software.
  3. Todos los cambios, o módulos que se vayan desarrollando en los sistemas deberán ser registrados en el sistema de control de versiones, donde los responsables del área deberán visualizar el nombre de los desarrolladores que subieron los cambios, la fecha y hora del cambio, y una breve descripción, todos estos datos para control interno del área.
  4. El sistema de control de versiones del código fuente de los sistemas será la fuente de respaldo al cual solo podrán acceder los desarrolladores de software, los administradores de Infraestructura Tecnológica y el Coordinador de Soporte Técnico y Desarrollo Tecnológico.
  5. El coordinador o coordinadora del área de Soporte Técnico y Desarrollo Tecnológico deberá informar mediante tarjeta informativa al Director de Red, Voz, Datos Imagen, de forma resumida los siguientes datos: el nombre de los sistemas que han tenido cambios, una breve descripción del sistema, el número de cambios que se le hicieron, y una breve justificación y descripción de dichos cambios. Este informe deberá realizarse de manera anual.

- **Respaldo de archivos de computadora:** Los archivos de computadoras son generados de manera rutinaria y cotidiana generalmente por software de ofimática (archivos de Word, Excel, PowerPoint, Access, pdf), que son compartidos por correo electrónico, o descargados de internet.

  Los archivos tienen grandes desventajas, entre las cuales podemos mencionar: son susceptibles a ser corrompidos por fallos del sistema (fallos de hardware o software), carecen de sistemas de recuperación, son propensos a la infección por virus, malware o ransomware, carecen de acceso

concurrente, la información es propensa a ser redundante, etc. Sin embargo las actividades de las áreas en muchas ocasiones ameritan su uso para el desarrollo de sus actividades.

Una de las estrategias que se sugieren para el almacenamiento de archivos es la implementación de carpetas compartidas, los accesos a dichas carpetas deben ser gestionadas mediante un dominio de directorio activo, para garantizar la seguridad y el acceso mediante políticas de dominio. Las carpetas compartidas deben ser almacenadas en un servidor especializado de almacenamiento que debe ser tolerante a fallos y altamente redundantes, para estos casos se puede implementar respaldos incrementales y en espejo con la finalidad de evitar la pérdida de los archivos.

Procedimientos para la ejecución de respaldos de archivos de computadora:

1. El administrador de infraestructura tecnológica deberá informar al Coordinador del área de Soporte Técnico y Desarrollo Tecnológico con copia Director de Voz, Datos e Imagen de manera anual mediante tarjeta informativa el número de carpetas compartidas que están contenidas en los servidores, su nombre, una breve descripción, el tipo de respaldo que ejecuta para dichas carpetas compartidas y la fecha del primer y último respaldo disponibles para restauración de dicha carpeta compartida.
2. En caso de que los archivos estén contenidos en los equipos de cómputo, y no en carpetas compartidas, un jefe de área o coordinador de área o director de área puede solicitar mediante tarjeta informativa al área de Soporte Técnico y Desarrollo Tecnológico el respaldo de la información de uno o varios equipos de cómputo de su área, indicando la fecha de ejecución del respaldo, o la periodicidad de la ejecución de los respaldos, el medio que utilizará para el almacenamiento de los respaldos y el nombre y cargo del responsable del resguardo de dicho medio de respaldo.
3. Si el respaldo de archivos de computadora es temporal por razones de mantenimientos no será necesaria una notificación por escrito, siempre y cuando se asegure la destrucción de la información respaldada al momento de restaurar los archivos al equipo. En caso de que se requiera que los respaldos no sean destruidos, entonces el director del área deberá elaborar un oficio al Director General del Centro de Control, Comando y Comunicación indicando el motivo del despaldo de la información, la descripción general de la información que se respalda, la fecha del respaldo, el nombre y cargo del responsable del resguardo del respaldo y el medio de almacenamiento del respaldo.

- **Respaldo de videos:** En el caso de los videos almacenados de la captura de imágenes mediante cámaras de video vigilancia, se sugiere almacenar un respaldo de la captura de las imágenes por el periodo que esté estipulado en las normas vigentes en materia de video vigilancia del Sistema Nacional de Seguridad Pública y El Secretariado Ejecutivo Nacional. El respaldo de dicha información deberá hacerse en servidores especializados que tengan tolerancia a fallos y que sean altamente redundantes para garantizar que no existan pérdidas de información. Para el caso de extracción de videos, dichos respaldo deberán realizarse en medios digitales que garanticen la persistencia de las imágenes y deberán generarse y manipularse con la implementación de cadenas de custodia de los medios.

Procedimientos para la ejecución de respaldos de videos de video vigilancia:

1. Para el caso de la extracción de videos y el respaldo de dicho contenido en medios de almacenamiento interno, el Centro Estatal de Emergencias deberá implementar un sistema de

cadena de custodia por escrito que involucre los procedimientos que se describen en los siguientes pasos.

2. Una entidad externa a C4 facultada deberá solicitar mediante oficio girado al Director General del Centro de Control, Comando y Comunicación la extracción de video de ciertas cámaras de video vigilancia, indicando la fecha y periodos de tiempo.
3. El Director General autorizará o denegará el acceso a dicha información según sus facultades.
4. En caso de que el Director General de C4 autorice la extracción del video girará copia de conocimiento del oficio donde soliciten la información al Director del Centro Estatal de Emergencias, quien instruirá a quien corresponda para la extracción de dicho video.
5. La información respaldada se almacenará en algún medio externo extraíble que proporcione el solicitante.
6. El Centro Estatal de Emergencias deberá llevar un registro en una cadena de custodia impresa el nombre de la persona que extrajo el video, el medio en el que se almacena el respaldo del video, los datos del oficio del solicitante, el o los nombres y cargo de los responsables que custodian dicho medio de almacenamiento que contiene el respaldo.
7. La cadena de custodia deberá tener visto bueno del director del Centro Estatal de Emergencias y del Director General del Centro de Control, Comando y Comunicación.
8. Se establecerá por escrito mediante un informe a través de tarjeta informativa dirigida al Director de Red, Voz Datos e Imagen, el cual se actualizará anualmente acerca del periodo de respaldo de los videos de las cámaras de video vigilancia, en caso de hayan cambios técnicos que alteren dicho periodo de respaldo, se debe actualizar dicho informe.

- **Respaldo de archivos de audio telefónico**: Los sistemas de telefonía implementados en el Centro Estatal de Emergencias respaldan los audios grabados de las llamadas del Call Center, con la finalidad de generar archivos de audio que se utilizan para establecer un control de calidad o para respaldo en caso de ser requerido por una instancia jurídica.

  Procedimientos para la ejecución de respaldos de audio de llamadas telefónicas:

  1. El Coordinador de telefonía informará anualmente mediante oficio o tarjeta informativa al director de la Red, Voz, Datos e Imagen el estatus de los respaldos de audios de telefonía que se resguardan en servidores especializados.
  2. En el informe anual incluyen los siguientes datos: Periodo de fechas respaldadas, el espacio de almacenamiento ocupado por el respaldo, la cantidad de archivos respaldados, las especificaciones de los tipos de archivos respaldados, el estatus del servidor de respaldo en cuanto a su capacidad de almacenamiento.
  3. En caso de no contar con un servidor de respaldo, se deberá informar anualmente las estrategias de seguridad que se implementan para mantener la integridad de los archivos almacenados y el estatus de los servidores o pólizas contratadas.
  4. Se establecerá por escrito mediante un informe a través de tarjeta informativa dirigida al Director de Red, Voz Datos e Imagen, el cual se actualizará anualmente acerca del periodo de respaldo de los videos de las cámaras de video vigilancia, en caso de hayan cambios técnicos que alteren dicho periodo de respaldo, se debe actualizar dicho informe.

Uso de Archivos computarizados:

En el caso del uso de la información que ya ha sido almacenada, esto para consulta, se podrá consultar el repositorio electrónicos con los que cuenta el C4 en cada una de las carpetas que han sido asignadas a cada una de las áreas y corporaciones, cabe señalar que los accesos a dichas carpetas están controladas por usuario, por lo que cual uso indebido de la dicha información quedará registrado en las bitácoras electrónicas de los sistemas.

b) Almacenamiento en área externa y medios de respaldo

Para todos los casos: respaldos de bases de datos, respaldos de código fuente de sistemas de información, respaldos de archivos de computadora, respaldo de videos, respaldo de audios de llamadas telefónicas; Si en alguno de los casos los respaldos se almacenen en áreas externas a las instalaciones del Centro de Control, Comando y Comunicación se implementarán las siguientes consideraciones:

1. Cada vez que se ejecute un respaldo, el responsable de la ejecución del proceso informará mediante oficio o tarjeta informativa a los directivos del área responsable de la información con copia al Director de la Red Voz Datos e Imagen notificando los medios de respaldos para guardar los archivos de respaldo, su ubicación física y el nombre del responsable del resguardo de dicho respaldo.
2. Cuando los respaldos se ejecuten de manera continua o con una frecuencia diaria, el responsable de ejecutar los respaldos implementará bitácoras donde lleve los registros de la fecha, hora, estatus del respaldo, el medio de almacenamiento, la ubicación física de los archivos de respaldo y el nombre del responsable del resguardo de dichos archivos de respaldo.
3. De la bitácora se extraerán los datos para realizar el informe anual con los datos descritos en el punto 1 de este apartado.
4. Cuando el almacenamiento de los respaldos se ubiquen fuera de las instalaciones el Centro de Control, Comando y Comunicación, el responsable de ejecutar los respaldo gestionará mediante tarjeta informativa dirigidas al Director de Red, Voz, Datos e Imagen, y el Director General de C4 para que se elabore y se firme un acuerdo de confidencialidad de la información con el área externa que almacena los archivos de respaldo.
5. Con la finalidad de garantizar la seguridad de los respaldos de información histórica de audios de llamadas del 911, de bases de datos, de archivos críticos, de extracciones de video de las cámaras de CCTV que ameriten ser respaldados, dichos respaldos deberán guardase en un área externa, el cual puede ser un servicio de almacenamiento de respaldos en la nube y/o un sitio secundario que se encuentre ubicado en una zona geográficamente distante del Centro de Control, Comando y Comunicación, para incrementar la seguridad, la integridad y el acceso de la información en caso de un desastre natural.

c) seguridad de los archivos de respaldo y los medios

Para todos los casos: respaldos de bases de datos, respaldos de código fuente de sistemas de información, respaldos de archivos de computadora, respaldo de videos, respaldo de audios de llamadas telefónicas; Es importante implementar seguridad en los archivos de seguridad.

1. Los archivos de respaldo externo cuyo contenido de información sea muy sensible y que sean almacenados en unidades de disco duro, memoria Flash USB, CD’s, u otros medios de almacenamiento extraíbles se recomienda aplicar un proceso de encriptación donde los archivos se segmenten en varios volúmenes o fragmentos, con la finalidad de que por separado no sean

legibles para los usuarios comunes. En caso de que este proceso se aplique en los archivos de respaldo, deberá ser informado al Director de Voz, Datos e Imagen y al Director General del Centro de Control, Comando y Comunicación en los informes anuales.

2. Para los casos de respaldos de información que su naturaleza sea la implementación de medios o dispositivos especializados, como servidores de bases de datos, servidores de almacenamiento masivo SAN, etc. Se debe implementar un control de acceso riguroso mediante la implementación de usuarios y contraseñas de administración. Para tales casos también se informará de forma anual al Director de Red, Voz, Datos e Imagen y al Director General del Centro de Control, Comando y Comunicación.

d) Destrucción de los archivos de respaldo y los medios.

Para todos los casos: respaldos de bases de datos, respaldos de código fuente de sistemas de información, respaldos de archivos de computadora, respaldo de videos, respaldo de audios de llamadas telefónicas; Se recomienda establecer por escrito, de manera oficial el tiempo o periodicidad de validez de los archivos de respaldo implementando las siguientes políticas:

1. Cuando los archivos se respalden en medios de almacenamiento masivo extraíbles, se recomienda llevar un registro de los respaldos, en dicho registro se incluirá el nombre de los archivos, la extensión que tienen, el medio de respaldo, la fecha de respaldo, el nombre del responsable de resguardo del respaldo, la ubicación física del medio de respaldo y la vigencia de su validez, de los registros se informará anualmente al Director de Voz, Datos e Imagen y al Director General de C4.
2. Cuando las vigencias de los archivos de respaldo se agoten, el responsable del área que ejecutó se procederá a la destrucción de la información, mediante el borrado o formateo de la unidad; Cuando se trate de información clasificada o muy sensible dependiendo del medio de almacenamiento se procederá a la destrucción del medio de almacenamiento, en el caso de memorias, CD's, DVD, Memorias SD o MicroSD. Dicho proceso debe ser informado mediante tarjeta informática al Director de la Red, Voz, Dato e Imagen.
3. Para los casos de respaldo de archivos, de bases de datos, o de información especializada en los que se emplean equipos especializados, como servidores de bases de datos, o servidores de almacenamiento masivo de información (SAN), se debe establecer en los informes anuales el periodo o vigencia de los respaldos, en la mayoría de los casos en se tipo de equipos los respaldos más antiguos se destruyen y se sobrescriben con respaldos más actualizados con la finalidad de optimizar el uso del almacenamiento. En estos casos se informará al Director de la Red, Voz, Datos e Imagen y al Director General del Centro de Control, Comando y Comunicación los periodos de borrado y sobre escritura de los respaldos más antiguos. Cuando se trate de información muy sensible se puede implementar la combinación con otros sistemas de respaldo, en dado caso también deberá anexarse dicha actividad en los informes.

RESPONSABLES

- El Director General del Centro de Control, Comando y Comunicación: Es el encargado de la canalización, gestión y autorización o en su caso también solicitar el respaldo de información de computadoras, de información almacenadas en bases de datos y en servidores de almacenamiento.

- El Director del Centro Estatal de Emergencias: Es el encargado de solicitar el respaldo de información de computadoras, de información almacenadas en bases de datos y en servidores del almacenamiento.
- El Director de la red de Voz, Datos e Imagen: Encargado de canalizar, autorizar o en su caso también solicitar el respaldo de información de computadoras, de información almacenadas en bases de datos y en servidores de almacenamiento.
- La Coordinación de Soporte Técnico y Desarrollo Tecnológico: Es la encargada de Canalizar las solicitudes de respaldo y ejecutarlas.
- Administradores de infraestructura
- Administradores de bases de datos
- Los usuarios finales de todas las áreas del Centro de Control Comando y Comunicación: Puede gestionar con sus mandos superiores el respaldo de su información en caso de requerirse, y están obligados a apegarse a los protocolos de la presente directiva.

Ing. Enrique Quinto Ceballos Aradillas
Director del Centro de Control, Comando y Comunicación C4
AUTORIZÓ

Lic. Osvaldo Alejandro Hernández León
Director de la red, voz, datos e imagen del Centro de Control, Comando Y Comunicación
REVISÓ

Capítulo	6. Operaciones	Subcapítulo	6.8 Sistemas de Computadoras
Número de directiva /Referencia CALEA		Fecha de elaboración	Fecha próxima revisión
		Agosto 2020	Agosto 2020
6.8.7 Acceso con Contraseña a Archivos o Sistemas de Información		Revisión:	
		2	
Alcance		Centro de Control, Comando y Comunicación C4	
Autoriza		Ing. Enrique Quinto Ceballos Aradillas Director General del Centro de Control, Comando y Comunicación.	

FUNDAMENTO LEGAL

- Código penal Federal artículo 211 Bis 1 a 6 y 400 bis.
- Ley federal de Derechos de autor (LFDA)
- Ley Federal de la Propiedad industrial (LFPI)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Norma ISO/IEC 27001 - Gestión de Seguridad de la Información
- Norma ISO/IEC 27002 – Estándar para la seguridad de la información.

OBJETIVO

Garantizar la integridad de la información contenida en sistemas de información del Centro de Control, Comando y Comunicación mediante la implementación de credenciales de acceso seguras basadas en las mejores prácticas establecidas en normas internacionales.

DESARROLLO DE LA DIRECTIVA

En el Centro de Control, Comando y Comunicación las diversas áreas que lo integran manejan sistemas de información para las actividades de rutina, principalmente en el Centro Estatal de Emergencias y los Centros de Control denominados C2, ubicados en las distintas regiones del Estado de Oaxaca. Los usuarios y contraseñas que se utilizan para el acceso a los diversos sistemas son gestionados mediante un Directorio Activo de Dominio, mediante el cual se establecen políticas de seguridad y de control de acceso. Dichas políticas solo se aplicarán a los sistemas críticos que manejan información sensible, como es el caso de los sistemas 089, 911 y correo electrónico institucional.

Procedimiento de creación de usuarios

Para todos los casos, se establecen las siguientes políticas de acceso a datos, archivos contenidos en equipos de cómputo o carpetas compartidas, sistemas de información, etc.

1. El Director o Directora del Centro Estatal de Emergencias, solicitará al Director de Red, Voz Datos e Imagen mediante tarjeta informativa o correo electrónico institucional, con copia de conocimiento al Director General del C4, en el cual se solicite los accesos nombrando los siguientes datos: Nombre completo del Sistema al que se le dará acceso, nombre completo del nuevo usuario, corporación a la que pertenece, rol que desempeñará en el sistema.
2. El Director de Red, Voz, Datos e Imagen, girará copia de conocimiento al Coordinador o Coordinadora de Soporte Técnico y Desarrollo Tecnológico, o Coordinadores que corresponda quienes ejecutarán la creación del usuario y contraseña.

3. En caso de que la solicitud de creación de usuarios y contraseñas sea para el acceso a otro tipo de sistemas que no involucren al Centro Estatal de Emergencias, la instrucción de creación será emitida mediante tarjeta informativa o correo electrónico institucional, por la Dirección General del Centro de Control, Comando y Comunicación hacia la Dirección de Red, Voz, Datos e Imagen, quien instruirá a la Coordinación que corresponda la generación de los accesos.
4. Todas las altas o bajas solicitadas por los encargados de los Sub Centro ubicados en las distintas regiones del Estado de Oaxaca deberán ser notificadas por Oficio, tarjeta informativa o correo electrónico institucional al Director del Centro Estatal de Emergencias, quien iniciará el proceso descrito en la presente directiva para la creación o de usuarios.
5. Una vez generados los usuarios y contraseñas se remitirán adjuntos en sobre cerrado por el conducto institucional en que fueron solicitados, por oficio, tarjeta informativa, o correo electrónico institucional en el caso de los encargados de los sub centros.

A continuación se establecen algunas consideraciones:

a. Construcción de contraseñas

- Los usuarios de acceso a sistemas de información, estarán compuestos por un nombre y uno de los apellidos del usuario, separados por un punto; Salvo en los casos que los altos mandos requieran una excepción a dicha política.
- Las contraseñas estarán compuestas por 8 caracteres de los cuales se deben contemplar por lo menos una letra mayúscula, una letra minúscula y un número

b. Cambios de contraseñas por lo menos cada 90 días

- Por políticas del Directorio Activo, todas las contraseñas de todos los usuarios de sistemas de información, acceso a archivos mediante carpetas compartidas, equipos de cómputo etc. caducarán cada 90 días.
- Una vez caducadas las contraseñas, se deberá solicitar el restablecimiento de la contraseña del usuario o usuaria siguiendo el proceso establecido al principio de la presente directiva.

c. Terminación del acceso con contraseñas cuando cambie la posición o condición de empleo

- Será responsabilidad total del Director o Directora del área en la que se desempeñe un usuario, el cual por cambio de adscripción, vacaciones, suspensión, separación laboral, o baja deje de desempañar sus funciones como subordinado del Director o Directora en dicha área
- Por tal motivo, el director o directora del área solicitará la baja de los accesos del usuario o usuaria mediante un conducto institucional: tarjeta informativa, oficio o correo electrónico institucional dirigido al Director de Red, Voz, Datos e Imagen, quien girará sus instrucciones a quien corresponda para ejecutar la baja del usuario en los sistemas.

RESPONSABLES

- El Director General del Centro de Control, Comando y Comunicación: Es el encargado de autorizar y girar la instrucción para la creación de usuarios y contraseñas o para las bajas de usuarios.
- El Director del Centro Estatal de Emergencias: Encargado de solicitar altas y bajas de usuarios de su dirección.
- El Director de la red de Voz, Datos e Imagen: Encargado de solicitar altas y bajas de usuarios de su dirección; Encargado de girar la instrucción a la coordinación que corresponda altas y bajas de usuarios.

- Todas las coordinaciones de las diversas áreas del Centro de Control, comando y Comunicación: Quienes se tienen que apegar a las recomendaciones de la presente directiva: Son las encargadas de dar de alta o baja usuarios a los diversos sistemas que administran.
- Coordinador de Soporte Técnico y Desarrollo Tecnológico: Son quienes ejecutan la creación y baja de usuarios en el Directorio Activo.
- Encargados de Sub Centros de las diversas Regiones del Estado de Oaxaca: Son quienes solicitan las altas o bajas de usuarios para sus sub centros.

Ing. Enrique Quinto Ceballos Aradillas
Director del Centro de Control, Comando y Comunicación C4
AUTORIZÓ

Lic. Osvaldo Alejandro Hernández León
Director de la red, voz, datos e imagen del Centro de Control, Comando Y Comunicación
REVISÓ