POLÍTICAS DE SEGURIDAD Y PROTECCIÓN EN SUCURSALES

REVISADO - 9 DIC. 2022

DICIEMBRE 2022

NOTA:

De conformidad con la NORMA MEXICANA NMX-R-025-SCFI-2015 EN IGUALDAD LABORAL Y NO DISCRIMINACIÓN, publicada en el Diario Oficial de la Federación el 19 de octubre de 2015, cuando se menciona algún cargo en el presente documento normativo del Organismo, se refiere indistintamente a mujer u hombre.

<table>
<tr><td colspan="3">I D E N T I F I C A C I Ó N</td></tr>
<tr><td colspan="2">Telecomm
TELECOMUNICACIONES DE MÉXICO</td><td>NÚM. DE REGISTRO:
TCM-9000-D03-22</td></tr>
<tr><td colspan="3">R E S P O N S A B L E S:</td></tr>
<tr><td>ELABORACIÓN, DISTRIBUCIÓN Y CONTROL:
DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA</td><td colspan="2">ACTUALIZACIÓN:
DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA</td></tr>
<tr><td>EXPEDICIÓN:
ABRIL DE 2015</td><td>LUGAR:
CIUDAD DE MÉXICO</td><td>FECHA:
DICIEMBRE DE 2022.</td></tr>
</table>

REVISADO - 9 DIC. 2022

Telecomm
TELECOMUNICACIONES DE MÉXICO

REGISTRO

NÚMERO: 465
TCM-9000-D03-22

NOMBRE DEL DOCUMENTO:

POLÍTICAS DE SEGURIDAD Y PROTECCIÓN EN SUCURSALES

FECHA Y NÚMERO DE REGISTRO: 465

DICIEMBRE 9 DEL 2022

DICIEMBRE DEL 2022

ÁREA QUE REGISTRA:

Mtro. Joaquín Hernández Vite
Gerente de Estadística y Normalización

EL DOCUMENTO "POLÍTICAS DE SEGURIDAD Y PROTECCIÓN EN SUCURSALES" TCM-9000-D03-22, QUEDA REGISTRADO CON EL NÚMERO 465, DE FECHA 9 DE DICIEMBRE DEL 2022.

CONFORME AL ESTATUTO ORGÁNICO DE TELECOMM:

ARTÍCULO 21, CORRESPONDE A LOS DIRECTORES,
FRACCIÓN XI.- ELABORAR Y ACTUALIZAR EL MANUAL DE ORGANIZACIÓN INSTITUCIONAL, DE PROCEDIMIENTOS, DE SERVICIOS Y LOS QUE SEAN COMPETENCIA DE SU UNIDAD ADMINISTRATIVA; Y ARTÍCULO 23, CORRESPONDE A LA DIRECCIÓN DE PLANEACIÓN, EVALUACIÓN E INFORMACIÓN INSTITUCIONAL,
FRACCIÓN XII.- COORDINAR CON LAS DIRECCIONES DE ÁREA LA ELABORACIÓN Y ACTUALIZACIÓN DE LOS INSTRUMENTOS NORMATIVOS DEL ORGANISMO;

REVISADO - 9 DIC. 2022

Telecomm
TELECOMUNICACIONES DE MÉXICO

AUTORIZACIÓN OFICIAL

NÚMERO
TCM-9000-D03-22

NOMBRE DEL DOCUMENTO:
POLÍTICAS DE SEGURIDAD Y PROTECCIÓN EN SUCURSALES

FECHA DE AUTORIZACIÓN:

DICIEMBRE DE 2022

MODIFICACIÓN No.3

DICIEMBRE DE 2022

AUTORIZÓ:

Lic. Adán García Zamora
Director de la Unidad Estratégica de Inteligencia

REVISÓ:

Lic. Geovanni Téllez Ávila
Subdirector de Seguridad, Investigación y Sistemas de Protección

ELABORÓ:

Ing. Alejandro Melo Bravo
Gerente de Monitoreo y Videovigilancia

REVISADO - 9 DIC. 2022

ÍNDICE HOJA

REVISADO - 9 DIC. 2022

REVISADO - 9 DIC. 2022

INTRODUCCIÓN

El presente documento modifica al documento "Políticas de Seguridad y Protección en Sucursales," con clave TCM-9000-D03-21 y registro número 440 de fecha 14 de diciembre de 2021.

De conformidad con lo dispuesto el artículo 29 fracciones I, II, III, V, VII, XI y XIV del Estatuto Orgánico de Telecomunicaciones de México, así como las funciones 1, 3, 4, 7, 9, 11 y 15 del Manual de Organización Institucional de Telecomunicaciones de México, la Dirección de la Unidad Estratégica de Inteligencia tiene la responsabilidad de establecer políticas, normas, procedimientos, sistemas y programas de seguridad actualizados, que eficazmente permitan prevenir y controlar conductas delictivas en contra de servidores públicos de la red de sucursales y de sus instalaciones.

Con la finalidad de mantener y mejorar la calidad de los diversos servicios que presta actualmente a sus clientes y usuarios, así como llevar a cabo procesos que permitan inhibir el incremento de ilícitos, como: robos (intrusiones), asaltos, faltantes en caja y extorsiones al patrimonio nacional por la delincuencia común y algunos servidores públicos, por lo que Telecomunicaciones de México se ve obligado a fortalecer las medidas de seguridad en la red de sucursales.

Las presentes Políticas de Seguridad y Protección, han sido elaboradas por instrucciones de la Dirección General de TELECOMM, tomando en cuenta los aspectos relacionados con la seguridad física y la protección de las sucursales, así como los lineamientos establecidos por la Dirección de la Unidad Estratégica de Inteligencia, desarrollando productos de inteligencia, planes y programas a través de trabajos de investigación, análisis, detección y prevención de conductas delictivas en contra de los empleados, usuarios, recursos e instalaciones de TELECOMM.

Es por ello, que en las presentes políticas se establecen los requerimientos necesarios para alcanzar el nivel de seguridad y protección en la red de sucursales, las cuales estarán a cargo de cada Gerencia Regional y/o Estatal y/o Jefaturas de sucursal, comprometiéndose a llevar a cabo en el ámbito de su competencia y responsabilidades, cada uno de los lineamientos de seguridad y prevención establecidos, así como cumplir con las prohibiciones estipuladas. También se definen los aspectos que deben ser cubiertos en forma genérica en cada instalación, adecuándolos con la disposición arquitectónica de cada inmueble, situación física, electrónica y condiciones del entorno, para cumplir adecuadamente con las disposiciones de seguridad y operación ordenadas.

De igual manera, se definen los medidas de seguridad que se deberán llevar a cabo en el manejo y traslado de valores, así como establecer límites de existencias de efectivo evitando las grandes concentraciones de dinero en áreas expuestas (ventanillas y cajas), para poder disminuir la probabilidad de siniestros y las pérdidas económicas no solo durante la realización del servicio sino antes y después del mismo, así como mejorar las actividades operativas y de seguridad aplicables durante la ejecución de programas sociales a fin de establecer las acciones correctivas, modificar, ampliar o establecer nuevas disposiciones de seguridad, que contrarresten las problemáticas que inciden de manera directa en el incremento de pérdidas durante la entrega de estos programas.

Por último, se definen las políticas para la información, capacitación y entrenamiento al personal en caso de siniestro o durante la comisión de un delito, conforme a la normatividad aplicable.

Este documento se integra por 3 apartados, el primero consta de Introducción, Marco Jurídico, Objetivo y Políticas Generales; el segundo apartado consta de 8 Capítulos los cuales se describen a continuación:

REVISADO - 9 DIC. 2022

CAPÍTULO PRIMERO, comprende conjunto de elementos físicos, electrónicos, normativos y operativos destinados a la protección de las sucursales, de sus trabajadores y del público usuario que asiste a ellas y del efectivo con el que operan.

CAPÍTULO SEGUNDO, este apartado establece medidas de seguridad, respecto a la solicitud y opiniones de seguridad respecto a la autorización de los límites en el manejo de recursos, autorización de pernoctas y traslado de valores.

CAPÍTULO TERCERO, comprende las medidas de seguridad aplicables durante el operativo de pago de los programas sociales.

CAPÍTULO CUARTO, se integra de las políticas, estrategias y programas en materia de seguridad e inteligencia que, la Dirección de la Unidad Estratégica de Inteligencia, como responsable propone, implementa y supervisa en coordinación con la Dirección de la Red de Sucursales, para garantizar el adecuado funcionamiento del Organismo.

CAPÍTULO QUINTO, describe el plan de atención a emergencias, en el que se establecen líneas de acción en caso de emergencia, como la ocurrencia del cierre o bloqueo de SIGITEL, corte de energía eléctrica, permanencia en la sucursal fuera de horario laboral por cargas de trabajo, apertura de una sucursal en días y horarios no laborales, asalto, robo por intrusión, actos fraudulentos, faltante en caja, amenaza de bomba, además del protocolo para reportar un ilícito.

CAPÍTULO SEXTO, consiste en la metodología para evaluar el nivel de riesgo de las sucursales por parte de la Dirección de la Unidad Estratégica de Inteligencia, con objeto de adaptar sistemas de disuasión, prevención o en su defecto, proponer la reubicación o cierre definitivo de sucursal, tomando como base las estadísticas de ilícitos registrados en cada entidad.

CAPÍTULO SÉPTIMO, enlista las medidas de seguridad que deberá adoptar el personal de la sucursal, así como todo el personal que tenga conocimiento de la información sensible sobre la operación de las sucursales.

CAPÍTULO OCTAVO, establece la coordinación entre la Dirección de la Red de Sucursales y la Dirección de la Unidad Estratégica de Inteligencia, con relación a la vigilancia y supervisión del tipo y nivel de riesgo a que están expuestas las sucursales, así como en la aplicación de medidas preventivas para brindar la seguridad necesaria.

Por último, el tercer apartado, el cual está integrado de los numerales IX. ANEXOS, contenido en el Capítulo Noveno, se integra por: Glosario de Términos, Formatos e Instructivos, Información Adicional (si procediera), y Control de Actualización del Documento.

REVISADO - 9 DIC. 2022

MARCO JURÍDICO

- CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.
  Publicada en el Diario Oficial de la Federación el 5 de febrero de 1917.
  Artículos 25, 28-párrafos cuarto y quinto, 90 y 134.
  (Última reforma publicada en el Diario Oficial de la Federación el 28 de mayo de 2021).

1.- LEYES

- LEY FEDERAL DE LOS TRABAJADORES AL SERVICIO DEL ESTADO, REGLAMENTARIA DEL APARTADO B) DEL ARTÍCULO 123 CONSTITUCIONAL.
  Publicada en el Diario Oficial de la Federación el 28 de diciembre de 1963.
  (Última reforma publicada en el Diario Oficial de la Federación el 18 de febrero de 2022).

- LEY FEDERAL DEL TRABAJO.
  Publicada en el Diario Oficial de la Federación el 1° de abril de 1970.
  (Última reforma publicada en el Diario Oficial de la Federación el 18 de mayo de 2022).

- LEY ORGÁNICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL.
  Publicada en el Diario Oficial de la Federación el 29 de diciembre de 1976.
  (Última reforma publicada en el Diario Oficial de la Federación el 9 de septiembre de 2022).

- LEY FEDERAL DE LAS ENTIDADES PARAESTATALES.
  Publicada en el Diario Oficial de la Federación el 14 de mayo de 1986.
  (Última reforma publicada en el Diario Oficial de la Federación el 1 de marzo de 2019).

- LEY DE INFRAESTRUCTURA DE LA CALIDAD
  Publicada en el Diario Oficial de la Federación el 1 de julio de 2020.

- LEY FEDERAL DE PROCEDIMIENTO ADMINISTRATIVO.
  Publicada en el Diario Oficial de la Federación el 4 de agosto de 1994.
  (Última reforma publicada en el Diario Oficial de la Federación el 18 de mayo de 2018).

- LEY DE SEGURIDAD NACIONAL.
  Publicada en el Diario Oficial de la Federación el 31 de enero de 2005.
  (Última reforma publicada en el Diario Oficial de la Federación el 20 de mayo de 2021).

- LEY FEDERAL DE PRESUPUESTO Y RESPONSABILIDAD HACENDARIA.
  Publicada en el Diario Oficial de la Federación el 30 de marzo de 2006.
  (Última reforma publicada en el Diario Oficial de la Federación el 27 de febrero de 2022).

- LEY FEDERAL DE SEGURIDAD PRIVADA.
  Publicada en el Diario Oficial de la Federación el 6 de julio de 2006.
  (Última reforma publicada en el Diario Oficial de la Federación el 17 de octubre de 2011).

- LEY GENERAL DE PROTECCIÓN CIVIL.
  Publicada en el Diario Oficial de la Federación el 6 de junio de 2012.
  (Última reforma publicada en el Diario Oficial de la Federación el 20 de mayo de 2021).

- LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.
  Publicada en el Diario Oficial de la Federación el 4 de mayo de 2015.

REVISADO - 9 DIC. 2022

(Última reforma publicada en el Diario Oficial de la Federación el 20 de mayo de 2021).

- LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.
  Publicada en el Diario Oficial de la Federación el 9 de mayo de 2016
  (Última reforma publicada en el Diario Oficial de la Federación el 20 de mayo de 2021)

- LEY GENERAL DEL SISTEMA NACIONAL ANTICORRUPCIÓN.
  Publicada en Diario Oficial de la Federación el 18 de julio de 2016.
  (Última reforma publicada en el Diario Oficial de la Federación el 20 de mayo de 2021)

- LEY GENERAL DE RESPONSABILIDADES ADMINISTRATIVAS.
  Publicada en el Diario Oficial de la Federación el 18 de julio de 2016.
  (Última reforma publicada en el Diario Oficial de la Federación el 22 de noviembre de 2021).

- LEY FEDERAL DE AUSTERIDAD REPUBLICANA.
  Publicada en el Diario Oficial de la Federación el 19 de noviembre de 2019.

2.- REGLAMENTOS

- REGLAMENTO DE LA LEY FEDERAL DE ENTIDADES PARAESTATALES.
  Publicado en el Diario Oficial de la Federación el 26 de enero de 1990.
  (Última reforma publicada en el Diario Oficial de la Federación el 23 de noviembre de 2010).

- REGLAMENTO DEL SERVICIO DE GIROS TELEGRÁFICOS.
  Publicado en el Diario Oficial de la Federación el 28 de noviembre de 2006.

- REGLAMENTO DE LA LEY FEDERAL DE SEGURIDAD PRIVADA.
  Nuevo Reglamento publicado en el Diario Oficial de la Federación el 18 de octubre de 2011.

- REGLAMENTO DE LA LEY FEDERAL DE ARCHIVOS.
  Nuevo Reglamento publicado en el Diario Oficial de la Federación el 13 de mayo de 2014.

- REGLAMENTO DE LA LEY GENERAL DE PROTECCIÓN CIVIL.
  Nuevo Reglamento publicado en el Diario Oficial de la Federación el 13 de mayo de 2014.
  (Última reforma publicada en el Diario Oficial de la Federación el 9 de diciembre de 2015)

- REGLAMENTO DE LA SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA.
  Publicado en el Diario Oficial de la federación del 30 de abril de 2019.

3.- DECRETOS

- DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSOS ARTÍCULOS DEL DECRETO POR EL QUE SE CREA EL ORGANISMO DESCENTRALIZADO DENOMINADO TELÉGRAFOS NACIONALES.
  Publicado en el Diario Oficial de la Federación el 14 de abril de 2011.

- DECRETO POR EL QUE SE APRUEBA EL PLAN NACIONAL DE DESARROLLO 2019-2024,
  Publicado en el Diario Oficial de la Federación el 12 de julio de 2019.

REVISADO - 9 DIC. 2022

4.- OTRAS DISPOSICIONES ADMINISTRATIVAS

- MANUAL DE ORGANIZACIÓN INSTITUCIONAL DE TELECOMUNICACIONES DE MÉXICO.
  Publicado en la Normateca Interna de Telecomunicaciones de México
  (Última actualización el 11 de agosto de 2022).

- MANUAL DE PROCEDIMIENTOS PARA LA OPERACIÓN DE SUCURSALES.
  El vigente publicado en la Normateca Interna de Telecomunicaciones de México.
  (Última actualización el 4 de marzo de 2020.)

- MANUAL DE PROCEDIMIENTOS DE LAS GERENCIAS REGIONALES Y ESTATALES.
  El vigente publicado en la Normateca Interna de Telecomunicaciones de México.
  (Última actualización el 20 de junio de 2022).

- CONDICIONES GENERALES DE TRABAJO DE TELECOMUNICACIONES DE MÉXICO.
  Las vigentes.

- CONDICIONES GENERALES PARA LA PRESTACIÓN DE LOS SERVICIOS DE TELECOMUNICACIONES DE MÉXICO.
  Aprobado conforme al Acuerdo No. 977 de la 105ª Junta Directiva celebrada el 19 de julio de 2013.

- ESTATUTO ORGÁNICO DE TELECOMUNICACIONES DE MÉXICO.
  Publicado en el Diario Oficial de la Federación el 14 de febrero de 2018.
  (Última actualización publicada en el Diario Oficial de la Federación el 1º de septiembre de 2021).
  Nota Aclaratoria publicada en el Diario Oficial de la Federación en 13 de octubre de 2021.
  Capítulo VII, Artículo 26, fracción XI.

- CÓDIGO DE CONDUCTA DE TELECOMUNICACIONES DE MÉXICO.
  Publicado en la Normateca Interna de Telecomunicaciones de México.
  Aprobado por el CEPCI el 25 de junio de 2019. Vigente.

- RESOLUCIÓN QUE REFORMA, ADICIONA Y DEROGA DIVERSAS DE LAS DISPOSICIONES DE CARÁCTER GENERAL A QUE SE REFIERE EL ARTÍCULO 95 BIS DE LA LEY GENERAL DE ORGANIZACIONES Y ACTIVIDADES AUXILIARES DEL CRÉDITO, APLICABLES A LOS TRANSMISORES DE DINERO A QUE SE REFIERE EL ARTÍCULO 81-A BIS DEL MISMO ORDENAMIENTO.
  Publicada en el Diario Oficial de la Federación el 20 de marzo de 2019.

- NORMA MEXICANA NMX-R-025-SCFI-2015 EN IGUALDAD LABORAL Y NO DISCRIMINACIÓN
  Secretaría de Economía. - Subsecretaría de Competitividad y Normatividad. - Dirección General de Normas. Publicada en el Diario Oficial de la Federación el 19 de octubre de 2015

- MANUAL DE CUMPLIMIENTO.
  El vigente publicado en la Normateca Interna de Telecomunicaciones de México.
  (Última actualización el 24 de junio de 2020.)

- MANUAL DE PROCEDIMIENTOS PARA LA ENTREGA DE APOYOS MONETARIOS A BENEFICIARIOS DE LOS PROGRAMAS SOCIALES, VIGENTE.
  Publicadas en la Normateca Interna de Telecomunicaciones de México.
  (Última actualización el 7 de abril de 2022).

- ACUERDO QUE REFORMA EL DIVERSO POR EL QUE SE EMITEN LAS DISPOSICIONES Y EL MANUAL ADMINISTRATIVO DE APLICACIÓN GENERAL EN MATERIA DE CONTROL INTERNO (MAAGM-CI).
  Publicado en el Diario Oficial de la Federación el 5 de septiembre de 2018.

- MANUAL PARA LA PROTECCIÓN CIVIL EN LA SECRETARÍA DE INFRAESTRUCTURA COMUNICACIONES Y TRANSPORTES.
  VIGENTE.

- MANUAL DE ORGANIZACIÓN DE LAS GERENCIAS REGIONALES Y ESTATALES.
  El vigente publicado en la Normateca Interna de Telecomunicaciones de México.
  Última actualización el 20 de junio de 2022

REVISADO - 9 DIC. 2022

OBJETIVO

Establecer las políticas y lineamientos que deberá observar el personal que integra la red de sucursales de TELECOMM, en materia de seguridad y protección, así como el establecimiento de los sistemas y recursos de seguridad que garanticen la vigilancia remota en la misma, fomentándolas como parte de su cultura y mística de servicio, encaminadas a orientar, unificar y prevenir la comisión de conductas ilícitas que afecten tanto al patrimonio institucional, así como la integridad física del público usuario y de los servidores públicos.

REVISADO - 9 DIC. 2022

POLÍTICAS GENERALES DE SEGURIDAD

Con el propósito de prever hechos delictivos como robos, asaltos, intrusiones, extorsiones y/o faltantes en caja (detectados por errores en la operación, quejas, entre otras) suscitados en las sucursales, el personal adscrito a estas deberá cumplir una serie de normas de seguridad que coadyuven a contener o provocar el fracaso del ilícito.

1. La Dirección de la Unidad Estratégica de Inteligencia en coordinación con la Dirección de la Red de Sucursales, se encargará de supervisar que las Gerencias Regionales y Estatales, así como sus coordinaciones y la persona a cargo de la sucursal, den cabal cumplimiento a las políticas de seguridad y protección en sucursales y de las sanciones que se emitan a los infractores.

2. Las Gerencias Regionales supervisaran que las Gerencias Estatales coordinen las actividades, disposiciones, normas, procedimientos de seguridad y vigilancia para su aplicación en las sucursales de su jurisdicción; conforme a las disposiciones que emita la Dirección de la Unidad Estratégica de Inteligencia.

3. Será responsabilidad de las Gerencias Regionales y/o Estatales supervisar que se cumpla con las disposiciones de seguridad y vigilancia en las sucursales de su adscripción.

4. La Dirección de la Unidad Estratégica de Inteligencia en coordinación con las Gerencias Regionales y Estatales establecerán un pliego de consignas específicas a desarrollar por el personal de seguridad y vigilancia, mismas que estarán diseñadas de acuerdo con las características propias de cada sucursal para el debido cumplimiento de los compromisos pactados.

5. Las Gerencias Regionales supervisaran que las Gerencias Estatales implementen la actualización de los directorios telefónicos de las autoridades, manteniéndolas en un lugar visible y a la mano.

6. El personal de las sucursales tiene estrictamente prohibido realizar cambio de dinero por diversas denominaciones a cualquier persona que solicite este tipo de servicios.

7. Será responsabilidad de la persona a cargo de la sucursal, recomendar y exhortar a su personal, para que durante su jornada laboral evite colocar el celular a la vista del público usuario, portar alhajas y/o artículos de valor ostentosos que llamen la atención, con el objeto de evitar agresiones a su integridad física en caso de asalto de acuerdo con lo dispuesto en el Capítulo IV, numeral 3.1 de las presentes políticas.

8. El personal de las sucursales deberá evitar la fuga de información sobre los procedimientos de operación, modalidades de transferencia de dinero, números de cuenta, claves de acceso y de seguridad, combinaciones de caja fuerte, horarios de recolección/entrega de valores y sumas que se manejan en cada una de ellas.

9. La persona a cargo de la sucursal, al término de sus labores deberá: cerrar las puertas y ventanas. En el caso de detectar vulnerabilidades reportar por escrito vía correo electrónico a su Gerencia Estatal correspondiente, los espacios desprotegidos por donde pudieran tener acceso las personas ajenas a esta, con el fin de que la Gerencia Regional y/o Estatal realice las gestiones necesarias para su pronta reparación, reforzando los accesos con protecciones metálicas en puertas y ventanas utilizando candados de seguridad donde se requiera.

REVISADO - 9 DIC. 2022

10. En caso de que la sucursal cuente con seguridad electrónica (cámara de video-vigilancia o panel de alarma), el titular al detectar el mal funcionamiento de los equipos, deberá reportarlo de inmediato a la Coordinación Técnica de la Gerencia Regional o Estatal para su pronta reparación en coordinación con la Gerencia de Monitoreo y Videovigilancia de la DUEI.

11. Si la sucursal cuenta con personal de vigilancia, el titular de esta deberá informarles sus responsabilidades y que tienen como principal objetivo vigilar la integridad física de los empleados, usuarios y bienes del Organismo, así como prevenir cualquier evento delictivo. Ver Capítulo I, punto 8.

12. Tratándose de la entrega de recursos económicos de programas sociales, así como de su proceso de ensobrado y traslado, la persona a cargo de la sucursal deberá mantener estricto hermetismo en el control de la información, inclusive a empleados que no tengan injerencia en el pago.

13. En caso de no contar con el apoyo de custodia armada para el desarrollo de programas sociales, la persona a cargo de la sucursal deberá suspender el proceso de recepción de remesas y de pago notificando inmediatamente a la Gerente Regional y/o Estatal, así como a la Dirección de la Unidad Estratégica de Inteligencia.

14. La persona a cargo de la sucursal deberá acatar estrictamente los límites de existencias de efectivo que se estipulen para cada sucursal, evitando las grandes concentraciones de dinero tanto en caja fuerte como en las ventanillas de servicio.

15. La persona a cargo de la sucursal deberá resguardar los recursos producto de los servicios telegráficos y/o los destinados para el pago de programas sociales al interior de la caja fuerte y/o cofre de seguridad, que en todo momento deberá estar debidamente cerrada y con la combinación corrida.

16. La persona a cargo de la sucursal al retirarse de las instalaciones, ya sea al término de su jornada laboral o para realizar alguna otra diligencia, invariablemente deberá asegurarse que la caja fuerte, puertas y ventanas permanezcan correctamente cerradas y el sistema de alarma se encuentre debidamente habilitado, con el fin de preservar la seguridad del numerario y las instalaciones; recomendando que los códigos para la operación del sistema de alarma sean personales y secretos. Si otro empleado requiere de estos, los deberá solicitar a la Gerencia Regional y/o Estatal a efecto de que lo autorice y le sean asignados por conducto del Centro Nacional de Monitoreo.

17. Las sucursales que cuenten con sistema local de alarma conectado a centrales de emergencia, este deberá ser operado y habilitado diariamente por personal previamente capacitado por la Gerencia Estatal; recomendando que los códigos para su operación sean personales y secretos. Si otro empleado requiere de estos, los deberá solicitar a la Gerencia Regional y/o Estatal a efecto de que lo autorice y le sean asignados por escrito.

18. La persona a cargo de la sucursal, a la conclusión de su jornada laboral, deberá cerciorarse que los dispositivos electrónicos de seguridad se encuentren en óptimo funcionamiento.

19. Los servidores públicos asignados en sucursales tienen estrictamente prohibido capturar fotografías o videos en el interior de estas, así como subir información a las redes sociales que vulnere la seguridad de las sucursales.

20. En el caso de que por motivo de una revisión de auditoría se presenten personas ajenas al Organismo, que pretendan ingresar a las instalaciones, el personal adscrito a las sucursales deberá confirmar con su Gerencia Regional y/o Estatal, la veracidad de la visita.

REVISADO - 9 DIC. 2022

Previo al ingreso y teniendo el documento de autorización a la vista, verificarán que sea un documento original, se encuentre firmado y que coincida plenamente con el informe previo que haya hecho la Gerencia o el personal que esta designe, a través de los medios institucionales disponibles.

El cuerpo del documento debe contener la autorización para que dichos auditores ingresen a la sucursal, en el día, fecha y hora señalada, deberá contener de manera detallada las actividades que realizarán el o los auditores, así como sus datos de identificación, mismos que deberán de cotejar con un documento de identificación original vigente.

Dichas visitas, deberán programarse y hacerse de conocimiento de la Dirección de la Unidad Estratégica de Inteligencia con la finalidad de llevar el registro y monitoreo de la visita a través de los medios tecnológicos disponibles.

21. El personal adscrito a la red de sucursales deberá acatar estrictamente las siguientes disposiciones en materia de seguridad informática vigentes y sus posteriores actualizaciones, mismas que la Gerencia de Seguridad Informática y Comunicaciones pone a su disposición en el portal interno del Organismo: Política de Seguridad de la Información, Política de Control Acceso, Política de Seguridad Física, Proceso de Control de Acceso Físico al Centro de Datos, Proceso ABC para Usuarios de Sistemas Operativos, Proceso ABC para Usuarios de Aplicaciones, Proceso ABC para Cuentas Privilegiadas, Proceso ABC para la Conexión de Usuarios a la Red de Datos Interna, Política De Seguridad Para Usuarios Finales, Política De Desarrollo De Software, Proceso De Abc Para La Conexión De Usuarios A La Red De Datos Interna y el BIA.
Dirección electrónica de consulta:
https://intranet.telecomm/portal/gsic/

REVISADO - 9 DIC. 2022

CAPÍTULO PRIMERO

I. MEDIDAS DE SEGURIDAD EN SUCURSALES.

1. MEDIDAS BÁSICAS DE SEGURIDAD.

Son el conjunto de elementos físicos, electrónicos, normativos y operativos destinados a la protección de las sucursales, de sus trabajadores y del público usuario que asiste a ellas y del efectivo con el que operan.

2. OBJETIVOS.

2.1 Disuadir la comisión de conductas ilícitas en contra del patrimonio del Organismo, servidores públicos y del público usuario, mediante el empleo de dispositivos de seguridad que eviten o minimice la materialización de un riesgo o amenaza y sus efectos.

2.2 Ofrecer un ambiente de confianza y tranquilidad al personal y al público usuario dentro de las sucursales.

2.3 Proteger los activos, el personal y al público usuario contra eventualidades delictivas o catastróficas provenientes de los fenómenos de origen natural que causen efectos dentro de las sucursales.

2.4 Asegurar la confidencialidad y disponibilidad de la información de acuerdo con su importancia y trascendencia, así como resguardar adecuadamente los activos informáticos.

2.5 Contar con la capacidad de respuesta adecuada, propia o de parte de las autoridades para atender una situación de alarma y para asegurar la continuidad de las operaciones de la sucursal, ante la ocurrencia de emergencias y/o diversas contingencias.

2.6 Minimizar los riesgos de quebrantos de origen fraudulento, facilitados por la omisión deliberada de algunos empleados.

3. ESTRATEGIAS DE SEGURIDAD Y PROTECCIÓN CONTRA CONDUCTAS ILÍCITAS.

3.1 PREVENIR.
Evitar factores de distracción con personas ajenas a la sucursal (amigos, familiares o compañeros), con alimentos, con celulares, tabletas, laptops, televisores, equipo de sonido, periódicos, audífonos, revistas, etc., y estar siempre atentos al entorno de la sucursal.

3.2 DISUADIR.
Desalentar la comisión de actos ilícitos mediante la aplicación de medidas de seguridad física, electrónica y operativa, así como aplicación de las respectivas medidas administrativas.

3.3 DEMORAR.
Obstaculizar, dificultar o retardar la comisión de una conducta ilícita a través de sistemas de seguridad.

3.4 DETECTAR Y ALERTAR.
Captar el momento del ilícito y generar una señal de alarma en el menor tiempo posible.

REVISADO - 9 DIC. 2022

3.5 IDENTIFICAR.
Reconocer el tipo de ilícito en forma rápida.

3.6 CANALIZAR.
Dirigir la información inicial del ilícito a la Gerencia Regional y/o Estatal para controlar la situación de manera oportuna.

3.7 REPORTAR INMEDIATAMENTE.
Poner en marcha los protocolos de respuesta para la atención del incidente y recuperar la normalidad perdida.

4. DISTRIBUCIÓN DE ÁREAS DE UNA SUCURSAL.

a) Acceso principal.
b) Área administrativa.
c) Área de caja fuerte y recuento de efectivo.
d) Zona de ambulatorio.
e) Ventanillas de servicios.
f) Área de bodega.

5. NIVEL DE SEGURIDAD REQUERIDO DE ACUERDO CON LAS ÁREAS DE CADA SUCURSAL.

La seguridad en cada una de las sucursales se basa en el principio de protección del objeto a resguardar. El sistema de protección se estructura mediante zonas concéntricas que van de mayor a menor nivel de seguridad a medida que nos alejamos del objeto a proteger.

Clasificación de las zonas sujetas a protección:

5.1 ZONA DE SERVICIO A CLIENTES O AMBULATORIO.

Zona donde el usuario no tiene restricciones de acceso, en la que normalmente se prestan servicios de atención y registro de operaciones (acceso principal).

5.2 ZONA PROTEGIDA.

Zona limitada por barreras físicas y de acceso controlado, en la que se ejerce una vigilancia sobre las operaciones, movimientos y permanencia de personas, tanto empleados como público usuario (ventanillas de atención al cliente, áreas de bodega y administrativa).

5.3 ZONA CRÍTICA.

Área de acceso restringido y delimitada por barreras físicas dentro de la zona protegida, en la cual la permanencia de personas es objeto de especiales medidas de control. Ejemplo de esta zona son: el área de caja fuerte y recuento de efectivo.

6. CRITERIOS PARA EL ESTABLECIMIENTO DE LAS MEDIDAS BÁSICAS DE SEGURIDAD.

En la red de sucursales a través de las Gerencias Regionales y/o Estatales, se deberán establecer e implementar las siguientes medidas de seguridad:

6.1 ENCRISTALAMIENTO DE VENTANILLAS.

REVISADO - 9 DIC. 2022

6.1.1 Definición.

Medida básica de seguridad implementada en las ventanillas de servicio, que consiste en la colocación de una barrera de protección física entre la zona de ambulatorio y la línea de cajeros, que tiene como objeto obstaculizar que personas ajenas ingresen a la zona protegida librando el mostrador de atención al público usuario.

6.1.2 Características de los cristales.

a) Deberá estar conformado por cristal de 6 mm. de espesor como mínimo, con película transparente.
b) Los cantos de los cristales deberán estar "boleados", para efectos de evitar astillamientos y lesiones, tanto a usuarios como a empleados.
c) Deberá contener una moldura, la cual debe ser de material resistente (madera, aluminio, herrería, etc.) y estar perfectamente fijada tanto en la base del mostrador como en la parte superior para fortalecer su nivel de resistencia y evitar su fácil derribamiento ante un ataque violento.

6.1.3 Colocación.

a) El mostrador de cajas deberá estar totalmente cerrado a lo largo y ancho de éste mediante el encristalamiento. En caso de existir separaciones entre cristal y cristal, será para el intercambio de documentos entre el personal y el público usuario, estas separaciones no deberán exceder de 15 centímetros de ancho cada una.
b) Las sucursales de nueva apertura o en remodelación, deberán contar con transfer (pasa documentos) tipo columpio.
c) Los cristales en las ventanillas deberán cubrir el vano del mostrador a la señalización de la ventanilla, o en su defecto a una altura mínima de 1.30 m. En caso de que exista espacio libre de la señalización al techo, deberá ser cubierto por algún tipo de material y/o protección de herrería previa solicitud del titular de la sucursal.

6.2 SEÑALIZACIÓN DISUASIVA Y LUGARES ÓPTIMOS PARA SU COLOCACIÓN.

6.2.1 Definición.

Son mensajes que se deben colocar en sitios estratégicos, con el propósito de advertir sobre las condiciones de seguridad y protección existentes, y su imposibilidad para verse afectadas o alteradas por el personal interno, de forma tal que disuadan la comisión de un delito.

6.2.2 Características de la señalización.

a) Se deberá colocar en lugares visibles para el público usuario en la zona de afluencia.
b) Debe poderse leer en condiciones normales de vista, a una distancia mínima de 3 metros.
c) La señalización en la zona protegida y crítica, deberá tener una medida mínima de 20 X 15 centímetros.
d) La señalización deberá ser de carácter permanente, elaborada profesionalmente, en material resistente al mal trato y al paso del tiempo y adherida en forma definitiva en los lugares seleccionados para cumplir con esta medida.
e) La señalización que por cualquier motivo muestre deterioro o información incompleta, deberá ser sustituida de inmediato para cumplir con el espíritu de esta.

REVISADO - 9 DIC. 2022

6.2.3 Colores de los letreros.

La Dirección de la Unidad Estratégica de Inteligencia en coordinación la Dirección de la Red de Sucursales, definirá los colores a utilizar en este tipo de señalización, se requiere que invariablemente sean seleccionados tonos que permitan atraer la atención del público usuario y del personal que labora dentro de las sucursales.

6.2.4 Para la colocación de la señalización se observará lo siguiente:

a) No deberán obstruir la visibilidad de las cámaras de video-vigilancia.
b) No deberá ser obstruida por algún otro aviso o elemento.
c) En los lugares donde exista mecanismo de retardo, deberá en forma obligatoria indicarse su existencia.
d) En las zonas protegida y crítica, deberán colocarse los dispositivos a los que haga referencia la señalización.

6.2.5 La señalización deberá contener textos y términos similares a los siguientes, según su colocación:

6.2.5.1 Señalización disuasiva y/o restrictiva en la puerta de acceso principal.

Se deberá colocar un letrero en la puerta principal, informando que, tanto el efectivo como valores que se encuentran dentro de las sucursales están bajo protección mediante sistemas de alarma automáticos enlazados a corporaciones policíacas.

6.2.5.2 Señalización disuasiva y/o restrictiva en las puertas de acceso para personal autorizado.

Se deberá colocar un letrero en cada una de las puertas que sean de acceso a las siguientes áreas:

a) Administrativa.
b) Área de caja fuerte y recuento de efectivo.
c) Ventanillas de servicios.
d) Área de bodega.
En el cual se indique que el acceso es únicamente para personal adscrito a la sucursal (personal autorizado).

6.2.5.3 Señalización disuasiva y restrictiva en áreas de manejo y custodia de efectivo.

En los mecanismos de retardo que se tienen instalados en las áreas de manejo y custodia del efectivo, se deberá colocar un letrero con una leyenda de advertencia que indique que el sistema que se tiene instalado para su protección, cuenta con mecanismos de retardo en la apertura, que impiden el acceso inmediato a éste y además, se encuentra conectada la apertura no autorizada con las corporaciones policíacas. Deberá advertirse que el personal de la sucursal, no tiene facultad para modificar o alterar estos dispositivos.

6.2.5.4 Señalización disuasiva en dispositivos electrónicos de seguridad y guarda de efectivo.

REVISADO - 9 DIC. 2022

Se deberá colocar un aviso en la zona de ambulatorio que a la vista del público usuario se indique, que el personal adscrito a la sucursal no tiene acceso a las áreas de caja fuerte y/o cofre de seguridad en la sucursal, ya que están protegidos por mecanismos de retardo en su apertura, que el tiempo programado para abrirse no depende de los empleados y que se encuentra bajo el Sistema de Operación de Video remoto.

6.2.5.5 Señalización disuasiva en dispositivos electrónicos de seguridad y monitoreo.

Se deberá colocar un aviso que indique que la sucursal se encuentra monitoreada bajo circuito cerrado conectado a seguridad pública, los 365 días del año, las 24 horas del día.

6.2.5.6 Señalización disuasiva de lineamientos de seguridad en la sucursal.

Se deberá colocar un aviso en la zona de ambulatorio que a la vista indique, que está prohibido en la vestimenta del público usuario el uso de accesorios que impidan captar el reconocimiento facial del mismo, por los sistemas de video vigilancia instalados en la sucursal (lentes, gorras, sombreros, etc.), así como el uso de dispositivos electrónicos que permitan tener contacto con personas externas que puedan vulnerar la seguridad (celulares, laptop, IPod, IPad, etc.)

7. DISPOSITIVOS ELECTRÓNICOS DE SEGURIDAD.

7.1 DEFINICIÓN.

Sistema de video-vigilancia destinado a proteger y controlar las áreas de mostrador, caja fuerte y/o cofre de seguridad, zona de recuento, zona de ambulatorio, zona de escritorio, perímetro y acceso a la sucursal, mediante el registro de imágenes, monitoreo y alertamiento en caso de emergencia, que funciona como elemento disuasivo a la delincuencia, como apoyo a las actividades de investigación de ilícitos por parte de la DUEI y de las autoridades correspondientes.

7.2 SISTEMAS INFORMÁTICOS BÁSICOS CON QUE DEBE CONTAR UNA SUCURSAL, SON LOS SIGUIENTES:

7.2.1 Sistemas de comunicaciones de datos de seguridad.

El sistema de comunicaciones de datos de seguridad, conecta a las sucursales con una central de monitoreo y de alarma, trasmitiendo las señales de alerta, fluyendo a través de un canal de comunicación.

7.2.2 Sistema de video-vigilancia.

a) Componentes.

El sistema de video de seguridad se compone de elementos electrónicos destinados al registro, grabación y transmisión de las imágenes secuenciadas que ocurren en las áreas controladas. Algunos de ellos son:

- Cámara de video de una sola posición.

REVISADO - 9 DIC. 2022

- Grabación de video digital de 24 hrs.
- Monitor o PC para mantenimiento correctivo, para colocación de cámara e imagen.
- Grabador de video local.
- Grabador de video centralizado.
- Canaleta para proteger todo el cableado instalado.

Estos sistemas permiten la grabación local o centralizada de las imágenes de un evento en curso y a su vez, apoyan la intervención de los cuerpos de respuesta al haberse presentado una situación crítica.

b) Características de las principales cámaras y alarmas.

- Cámaras analógicas (CCTV EverFocus 400 y 410 y EPCOM, grabadores de video digital compactado de 4 canales): Tienen un grabador digital local tipo DVR (digital video recorder), el área Técnica designada por cada Gerencia Regional y/o Estatal, coadyuvará para la obtención del video mediante los medios necesarios para esto.

- Cámaras digitales IP: Mobotix y Axis son cámaras que emiten las imágenes directamente a la intranet o internet sin necesidad de un ordenador, se conecta y alimenta por medio del Power-Over-Ethernet PoE). La Dirección de la Unidad Estratégica de Inteligencia, será el área responsable de recuperar las imágenes y enviarlas a las Gerencias Regionales y/o Estatales, para realizar las gestiones necesarias ante las instancias legales que corresponda previa solicitud de éstas.

- Alarmas remotas TELCO/IP: Vista 48LA (es un panel híbrido que ofrece 64 zonas, de las cuales 56 pueden ser inalámbricas, ofrece incluso la posibilidad de definir sus propias funciones de zona funcional local y remota), VISTA 10 (es un panel de control más versátil, cuenta con 6 zonas y da la posibilidad de enviar señales de alarma, así como de carga/descarga a través de un protocolo de Internet) y DSC (es un panel que ofrece 4 zonas cableadas, con doblaje a 8 supervisado, expansión a 8 zonas mediante zona extra del teclados), son paneles de alarmas. La Dirección de la Unidad Estratégica de Inteligencia, será la responsable de supervisar y controlar las activaciones y señales de los dispositivos en referencia.

- Alarmas locales: Son los dispositivos que requieren atención en la sucursal, no son monitoreadas por el Centro Nacional de Monitoreo y funcionan como disuasivas. En este caso la Gerencia Regional y/o Estatal, será la responsable de su funcionamiento y operación.

c) Ubicación.

Las cámaras de video-vigilancia deberán colocarse considerando los siguientes objetivos:

REQUERIMIENTO DE COBERTURA	OBJETIVO
Cubrir la zona de entrada principal.	Registrar la presencia del público usuario que ingrese al área de ambulatorio.
Cubrir la zona de ambulatorio.	Registrar las acciones de la zona de atención a clientes o de ambulatorio: tránsito y estadía de las personas.

REVISADO - 9 DIC. 2022

Cubrir las ventanillas de servicios o zonas de manejo y custodia de efectivo.	Registrar las acciones en la zona protegida.
Cubrir el área donde se encuentre la Red de Telecomunicaciones.	Proteger las áreas sensibles de TELECOMM para garantizar la continuidad de las operaciones.

Colocación y número de cámaras del sistema de video-vigilancia en función del número de ventanillas que operan:

		CÁMARAS			
No. Ventanilla	Nivel de exposición	En ventanillas	En zona de ambulatorio	Zona crítica	Total
1	Bajo	1	1	1	3
2	Bajo	1	1	1	3
3	Medio	2	1	1	4
4	Medio	2	1	1	4
5	Medio	2	1	1	4
6	Alto	3	1	1	5
7	Alto	3	1	1	5
8	Alto	3	1	1	5
Más de 9	Crítico	1 por cada 3	1	1	5

d) Procedimiento para la obtención de imágenes del sistema de video-vigilancia.

- Caso 1. Grabadores digitales (DVR´s)

  El coordinador o responsable técnico designado por las Gerencias Regionales y/o Estatales para esta labor, se presentará en la sucursal con el fin de conectar un dispositivo de captura de video en la salida del DVR o por el medio que tenga, para la obtención de imágenes, mismas que servirán para entregarlas a las instancias legales correspondientes y también las enviará a la Dirección de la Unidad Estratégica de Inteligencia, en un plazo no mayor a 48 horas hábiles, para su análisis correspondiente.

- Caso 2. Sistema de video-vigilancia IP.

  La Dirección de la Unidad Estratégica de Inteligencia, por medio de la Gerencia de Monitoreo y Videovigilancia pondrá a disposición de las Gerencias Regionales y Estatales, las imágenes captadas por los sistemas de video-vigilancia sobre los incidentes que ocurran en las sucursales, cuando exista solicitud previa de una instancia legal o a petición especifica de la Dirección de la Red de Sucursales, misma que deberá estar fundada y motivada.

7.2.3 Sistema de Monitoreo y Alarma de Seguridad.

El sistema informático de monitoreo y alarmas de seguridad consta de diversos dispositivos electrónicos destinados a la generación y gestión local o remota de las señales de alarma, mediante la revisión cíclica del estatus de los sensores instalados en las áreas protegidas.

REVISADO - 9 DIC. 2022

El objetivo de estos elementos es prevenir, detectar, minimizar y eliminar la probabilidad de la realización de ilícitos o siniestros, con sus consecuencias y reducir la vulnerabilidad de las instalaciones.

7.2.3.1 Elementos.

Los elementos que integran el Sistema de Monitoreo y Alarma de Seguridad y que pueden ser colocados en forma alternativa, siempre y cuando se tenga la capacidad institucional, pero sin dejar de cubrir ninguno de los puntos vulnerables, tienen los siguientes propósitos de acuerdo con su objetivo y ubicación:

DISPOSITIVO	OBJETIVO	UBICACIÓN
Botonera de asalto.	Emitir una señal de alarma a la central de monitoreo en el momento en que son activados manualmente.	En ventanilla y en la zona crítica.
Sensor de apertura y cierre.	Emitir una señal de alarma en el momento que se abre o cierra alguna puerta y se encuentre armado el sistema.	En puertas de acceso y caja fuerte y/o cofre de seguridad.
Sensor de movimiento.	Emitir una señal de alarma cuando se detecte algún movimiento en la zona protegida y se encuentre armado el sistema.	Los necesarios para cubrir la zona de influencia y crítica.
Sensor de ruido.	Emitir una señal de alarma cuando se intenta perforar el dispositivo.	Caja fuerte y/o cofre de seguridad.
Sensor de temperatura.	Emitir una señal de alarma cuando se incrementa espontáneamente el nivel de temperatura en la zona protegida.	Caja fuerte y/o cofre de seguridad.
Sensor de humo.	Detectar la presencia de humo en el aire y emitir una señal acústica avisando del peligro de incendio.	Área de bodega donde se concentra el archivo.
Sensor de vibración.	Detectar vibraciones generadas por movimiento, que puede presumir la tentativa de penetrar a la sucursal.	Puertas y ventanillas.
Sirena exterior.	Emitir una señal audible local de alto nivel de decibeles cuando el sistema de alarma se ha activado por una señal de intrusión.	En el exterior de la sucursal.
Control local de monitoreo y alarma.	Recibir las señales de alarma locales y retransmitirlas a la central de alarmas.	En la zona de ambulatorio y protegida.
Respaldo de energía. (batería)	Garantiza la continuidad de la operación de los sistemas ante una interrupción del suministro eléctrico.	Con capacidad suficiente para cubrir una hora sin energía, colocado en la zona de ambulatorio y administración.
Magnetos (Sistema de imanes).	Emite señal de alarma,	Se instala en puertas de acceso principal, cuarto de recuento, caja fuerte, etc.

REVISADO - 9 DIC. 2022

7.2.3.2 Tipo de señales que monitorea.

a) Asalto.
b) Intrusión o Robo.
c) Amago.

7.2.3.3 Las sucursales deben contar con lo siguiente:

a) Sistemas de seguridad y protección que permitan la colocación de sensores periféricos en lugares estratégicos, como lo son:

- Ambulatorio o área de servicio a clientes.
- Ventanillas o cajas de servicios a clientes.
- Área de caja fuerte principal y/o cofre de seguridad.
- Área de oficina de administrador o recepción de efectivo.
- Botones de asalto en el área de ventanillas.
- Botón inalámbrico de emergencia en las áreas que se consideren.
- Sirena y luz estroboscópica dentro de la sucursal.

Es importante que estén conectados al Centro Nacional de Monitoreo de la Gerencia de Monitoreo y Videovigilancia del Organismo y de ser posible a las comandancias o centrales de policía de su localidad.

b) Sistemas de monitoreo que permita registrar, transmitir y recibir señales de alarma en tiempo real y en forma simultánea interconectarse al Centro Nacional de Monitoreo de la Gerencia de Monitoreo y Videovigilancia, en el momento en el que tenga lugar un siniestro, se presuma la comisión de un delito por el empleado de la sucursal o bien que el personal de una unidad remota accione el sistema de alarma.

c) Sistemas informáticos de comunicación, de video o grabación de imágenes u otros sistemas tecnológicos que permitan captar, grabar, registrar y transmitir en forma simultánea, las escenas y los hechos ocurridos, con el objeto de coadyuvar a la prevención de conductas ilícitas e identificación de los probables responsables, así como las causas en casos de siniestros.

El Centro Nacional de Monitoreo, recibirá las señales de alarma y la transmisión de imágenes de las cámaras de video-vigilancia; con lo que implementará los actos tecnológicos y convencionales que permita a los cuerpos de seguridad pública acceder a dichas señales, en las mismas circunstancias y en tiempos equivalentes.

d) Control local de alarmas.

Es el elemento fundamental de la instalación, en el cual se tienen que producir las señales necesarias, ante los cambios de estado de los detectores asociados al sistema.

REVISADO - 9 DIC. 2022

7.2.4 Mecanismos de retardo en el acceso a las áreas de manejo o guarda de valores y efectivo.

7.2.4.1 Características de los mecanismos de retardo y su aplicación.

Estos mecanismos están integrados a controladores de aperturas como pueden ser un dispositivo de acceso digital electrónico o una chapa electrónica. Sus tiempos de retardo deberán programarse de acuerdo con el tipo de dispositivo y la finalidad de la seguridad y protección que persigan: En cajas fuertes, se tendrá un tiempo mínimo de 5 minutos (En este dispositivo se guarda la mayor parte del efectivo y su utilización es programable con base en los requerimientos típicos de las ventanillas).

7.2.4.2 Botón de liberación o mecanismo similar para su apertura.

Son dispositivos físicos y electrónicos que tienen la función de abrir una puerta de seguridad (puerta de ante para cajas fuertes) con un retardo previamente programado. Estos dispositivos se deben instalar en el acceso a las áreas de manejo de efectivo o guarda de valores - efectivo de manera alternativa, con el propósito de retardar su apertura y reducir el nivel de exposición y disuadir cualquier ataque.

7.2.5 Dispositivos y mecanismos de respaldo para los sistemas.

Para la operación adecuada de los sistemas informáticos, de seguridad y protección dispuestos en las sucursales de TELECOMM, se debe contar con dispositivos y mecanismos de respaldo que aseguren su continuidad operativa ante la interrupción inesperada del suministro eléctrico, como son las baterías con capacidad de operación autónoma de por lo menos 30 minutos, ante la interrupción inesperada del suministro eléctrico.

7.3 ALMACENAMIENTO LOCAL Y REMOTO.

Grabadores locales tipo DVR, estos dispositivos tendrán capacidad de almacenamiento de la siguiente manera: grabadores modelo EDSR400h máxima resolución e imágenes por segundo contendrán hasta 48 horas de grabación; grabadores modelo EDR410h podrán grabar hasta 10 días a máxima resolución e imágenes por segundo.

Cabe señalar, que en el caso del Sistema Mobotix y AXIS, se podrán almacenar de manera local por un periodo de tres días, la capacidad en los servidores de almacenamiento del Centro Nacional de Monitoreo será de una imagen por minuto un periodo máximo de un mes.

7.4 MANTENIMIENTO A EQUIPOS ELECTRÓNICOS DE SEGURIDAD.

La Dirección de la Unidad Estratégica de Inteligencia supervisará el debido cumplimiento de las Gerencias Regionales y Estatales al Programa Anual de Mantenimiento Preventivo para los equipos electrónicos de seguridad instalados en las sucursales, el cual deberá ser enviado por estas a la Gerencia de Monitoreo y Videovigilancia durante la primera quincena del mes de diciembre para aplicarse en el año siguiente, con la finalidad de garantizar su seguimiento, el buen funcionamiento y operación de estos.

REVISADO - 9 DIC. 2022

a) Grabadores digitales.
Mantenimiento preventivo, grabador de video (DVR), cámara (s), ajuste, enfoque y dirección de lentes, ajuste de sistema (hora y fecha). Previa autorización de la referida área.

b) Sistema de video-vigilancia.
Mantenimiento preventivo, cámara IP (limpieza de domo y NAS), ajuste, enfoque y dirección de lentes, ajuste de sistema (hora y fecha). Previa autorización de la referida área.

c) Alarmas remotas.
Mantenimiento preventivo, panel de alarma, sensores de movimiento, botón inalámbrico y fijo de pánico, bocina, verificación de funcionamiento de los dispositivos antes señalados en la central de alarmas del Centro Nacional de Monitoreo.

d) Alarmas con funcionamiento local.
Mantenimiento preventivo, panel de alarma, sensores, botón fijo de pánico, bocina, verificación de funcionamiento de los dispositivos antes señalados localmente.

7.4.1 Confirmación número de reporte.

Cuando se realicen quincenalmente los trabajos de mantenimiento correctivo al sistema de video-vigilancia, los encargados de esta labor en cada Gerencia Regional y/o Estatal, solicitarán confirmación del funcionamiento y operación de los equipos que presenten fallas a la Gerencia de Monitoreo y Videovigilancia, dependiente de la Dirección de la Unidad Estratégica de Inteligencia a los números telefónicos 5510350248 y 55 50 90 11 00 Ext. 4244, 4247, 4249 y 4262. Dicha Gerencia emitirá un reporte para cualquier aclaración.

7.4.2 Retiro de equipo para mantenimiento correctivo.

En caso de que el equipo de video-vigilancia no responda a las pruebas básicas y se requiera retirar de la sucursal, el Coordinador técnico de la Gerencia Estatal deberá remitir mediante correo electrónico, una solicitud de autorización para el retiro de los equipos, posteriormente, el técnico habilitado por la Gerencia Regional y/o Estatal, realizará vía telefónica a la Gerencia de Monitoreo y Videovigilancia de la Dirección de la Unidad Estratégica de Inteligencia, la confirmación para poder proceder al retiro del equipo. El técnico que atiende la llamada le proporcionará un número de confirmación de retiro para cualquier aclaración.

7.4.3 Capacitación.

La Dirección de la Unidad Estratégica de Inteligencia, a través de la Gerencia de Monitoreo y Videovigilancia, en coordinación con las Gerencias Regionales y Estatales, elaborarán un programa anual de capacitación técnica, para la instalación y mantenimiento de los dispositivos electrónicos de seguridad, impartidos por personal del área de Monitoreo o por una compañía externa.

8. PERSONAL DE VIGILANCIA.

En aquellas Gerencias Regionales y/o Estatales que cuenten con servicios de vigilancia contratados para las sucursales, deberán solicitar al prestador de los servicios, las siguientes medidas básicas indispensables.

8.1 El personal de vigilancia deberá ceñirse únicamente a las funciones que le competen y permanecer en la sucursal alerta y observando durante todo el tiempo que esta permanezca abierta al público usuario.

8.2 Llevar a cabo un estricto control de inspección del área, sin permitir en ningún momento que la confianza, el cansancio o fatiga aminore la labor de inspección, manteniendo una sobre vigilancia y supervisión permanente.

8.3 Se solicitará a los elementos de vigilancia que deberán estar siempre alerta de cualquier extraño que se encuentre en las inmediaciones de la sucursal, especialmente en automóviles estacionados cerca de la puerta de acceso y personas sospechosas que merodeen en la zona.

8.4 Identificar y conocer ampliamente los accesos, las zonas vulnerables y el ambiente externo de la sucursal, esto es:

a) Situación geográfica (colonia, barrio, poblado, comunidad, vías de acceso, etc.).
b) Número de accesos al inmueble (puertas frontales, traseras, ventanas, estacionamiento).

8.5 Deberá elaborar y entregar a la persona a cargo de la sucursal un parte de novedades diariamente.

8.6 Si la sucursal cuenta con servicio recolector de valores, el personal de vigilancia deberá estar atento de que se lleve a cabo de manera segura.

8.7 Si la empresa prestadora de servicios de recolección de valores realiza cambios y/o sustitución de su personal, deberá identificarlos plenamente antes de poder otorgarles facilidades para ingresar a la sucursal y solicitará al administrador que verifique la autenticidad de las credenciales del personal vía telefónica con la propia empresa y el titular de la Gerencia Regional y/o Estatal, tomando en consideración el catálogo de firmas y fotografías que la ETV emite.

8.8 Identificará a las corporaciones policiacas de la localidad y servicios de emergencia, a fin de agilizar el reporte de ilícitos.

8.9 Las sucursales que cuenten con estacionamiento para el personal, deberán:

a) Identificar al personal que ingresa.
b) Registrar la entrada y salida en el parte de novedades.
c) Revisar el interior, exterior y cajuela del vehículo.

8.10 Deberán solicitar pase de salida de todo tipo de bienes muebles, cosas u objetos que ingresen o salgan de la sucursal, verificando que la firma sea la autorizada para este fin.

8.11 El personal de vigilancia deberá estar capacitado en los siguientes aspectos:

a) Manejo y control de detectores de metales fijos y manuales, gas lacrimógeno, toletes, vehículos motrices y equipo de radiocomunicación propiedad del prestador de servicios, que garanticen una total y completa intercomunicación para auxiliar en las labores de vigilancia.
b) Debe conocer el uso y manejo de armamento, manejo defensivo y evasivo.
c) Prácticas de tiro.
d) Defensa personal.
e) Primeros auxilios.

REVISADO - 9 DIC. 2022

f) Normatividad en los procesos de recolección y entrega de valores.
g) Protección civil.
h) Planes de reacción en casos de emergencia.
i) Identificación de sospechosos.

8.12 El personal de seguridad deberá portar arma de fuego, ya que además de ser un elemento disuasivo le permite reaccionar ante cualquier eventualidad. Además, deberá llevar a cabo las siguientes acciones:

a) Evitar desórdenes.
b) Regular el tránsito de clientes en el ambulatorio, para evitar aglomeraciones y que no se obstruyan los lugares de acceso a las sucursales.
c) Llamar la atención de los que transgredan alguna norma establecida por la sucursal de carácter general (no fumar, no hacer uso de celulares, no usar gorra y sombrero, casco, lentes oscuros o cualquier prenda que cubra su rostro y dificulte su identificación, formar filas a distancia segura de las cajas, no merodear alrededor de la sucursal sin motivo, aguardar ordenadamente en los lugares asignados para ser atendidos por trámites diversos, alertar sobre personas sospechosas, etc.)
d) Deberá evitar el acceso a vendedores ambulantes, personas en situación de calle, etc.
e) Verificar la presentación de documentos oficiales de identificación a las personas que argumenten ser técnicos en reparación o similares, que se pretendan dirigir al interior de la sucursal, asimismo, pedirá la autorización del personal encargado para su acceso.
f) Revisar todo paquete sospechoso que sea ingresado por visitantes o personal del servicio y reportarlo a la persona a cargo de la sucursal para verificar su procedencia.
g) En caso de rolarse el personal de vigilancia, deberán dejar por escrito todas las consignas pendientes para que el guardia entrante las pueda realizar y tenga pleno conocimiento de todas las situaciones que se le puedan presentar. Cualquier inconveniente que se presente será responsabilidad del que entregó el turno, sino hubiese dejado la respectiva consigna por escrito.
h) Conocer y distinguir a cada uno de los empleados de la sucursal, así como los vehículos y sus placas.
i) Informar de maltratos a las cerraduras o a las estructuras y abuso de estas.
j) Conocer las zonas de riesgo en la sucursal y mantener constante observación de éstas en horas más concurridas de la operación.
k) Conocer y ubicar los equipos de emergencia tales como extintores, hidrantes, elementos de contra incendio, fusibles o tacos eléctricos, dándoles el uso adecuado.

8.13 Se le instruirá al vigilante, que deberá de colaborar con las medidas de racionalización, con acciones como:
a) El apagado de iluminación en zonas que no se esté laborando.
b) Cierre de llave de agua en el baño.

8.14 El personal designado para la prestación del servicio de vigilancia, se presentará con anticipación para vigilar y custodiar que la persona a cargo de la sucursal realice la apertura sin contratiempos y así iniciar puntualmente su servicio, debidamente equipado y uniformado, este personal deberá estar capacitado para atender eficientemente el servicio y acatar las consignas establecidas.

8.15 Cada Gerencia Regional y/o Estatal establecerá los mecanismos para garantizar la asistencia del personal y el cumplimiento estricto del alcance de los servicios de vigilancia en las condiciones programadas, en este sentido, designará a los servidores públicos que consideren necesarios para efectuar tareas de supervisión de los servicios. Adicionalmente, se deberá

REVISADO - 9 DIC. 2022

obtener un contrato que permita alcanzar el máximo grado de eficiencia y optimización del servicio, que redunde plena confiabilidad de la seguridad contratada. El prestador de servicios deberá comprometerse expresamente a cubrir diariamente y por turno el número de elementos que propone y cotiza, en su propuesta.

8.16 El prestador de servicios deberá garantizar que el personal que contrata y que será asignado para la prestación del servicio, no cuenten con antecedentes penales, ni estén sujetos a procesos penales por delitos culposos, tengan buena conducta, no hagan uso de sustancias psicotrópicas, estupefacientes u otros. Además, deberá realizar validaciones personalizadas de los datos proporcionados por el aspirante.

8.17 Es importante que el prestador de servicios de vigilancia cuente con equipo de radiocomunicación y vehículos de supervisión exclusivos para las necesidades del servicio.

9. MEDIDAS ADICIONALES A LAS MEDIDAS BÁSICAS DE SEGURIDAD.

Con base en las deficiencias detectadas por el personal adscrito a las sucursales, las Gerencias Regionales y Estatales a través del personal adscrito a las sucursales y de la detección de deficiencias en las instalaciones cada una de las sucursales promoverá la adopción de medidas de seguridad adicionales, que fortalezcan su nivel de protección, las cuales deberán contribuir a los siguientes aspectos:

9.1 Control de accesos.

Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.

9.2 Manejo y protección del efectivo.

Se pueden implementar dispositivos para la protección de efectivo y valores con mecanismo de retardo físico o electrónico incorporado. En su defecto, el área donde se ubique el dispositivo blindado para la protección deberá contar con un mecanismo de acceso con retardo físico o electrónico.

9.3 Protección a los datos personales.

El personal que se encuentra en las ventanillas de servicio solo podrá tratar los datos personales que sean estrictamente necesarios para efectuar cualquier trámite, ya que los usuarios tienen derecho a la protección de los datos personales sobre las operaciones que realicen en las sucursales.

REVISADO - 9 DIC. 2022

CAPÍTULO SEGUNDO

II. NORMATIVIDAD SOBRE MÉTODOS Y LÍMITES EN EL MANEJO Y TRASLADO DE VALORES.

1. OBJETIVOS.

1.1 Establecer políticas y medidas de seguridad en el manejo y traslado de valores, así como límites de existencias de efectivo en sucursales evitando grandes concentraciones de dinero en las sucursales y específicamente en áreas expuestas (ventanillas y cajas), para disminuir la probabilidad de pérdidas económicas elevadas.

1.2 Celebrar acuerdos de colaboración con dependencias y entidades de los tres niveles de gobierno, (Federal, Estatal y Municipal), encaminados a reforzar los esquemas de seguridad implantados en las sucursales y en el desarrollo de sus labores, a fin de minimizar el riesgo de la materialización de un evento delictivo; así como velar por la integridad física de los servidores públicos, usuarios y de los recursos del Organismo.

2. LÍMITE EN LAS EXISTENCIAS DE EFECTIVO EN LAS SUCURSALES.

Es una medida de seguridad que permite reducir el nivel de pérdidas ante la ocurrencia de un evento delictivo. Consiste en acotar las existencias de efectivo en la caja fuerte y/o cofre de seguridad y en las ventanillas de servicios, de tal manera que el efectivo real expuesto por la actividad de la sucursal se encuentre dentro de límites autorizados.

Los límites de efectivo en las sucursales deben ser difundidos a través de la Dirección de la Red de Sucursales de acuerdo con la normatividad interna de la Institución y conforme a los dispuesto en el numeral 2.2.7 Procedimiento para el visto bueno de seguridad para la asignación de montos en caja en las sucursales del Manual de Procedimiento de la DUEI vigente.

2.1 Límite de efectivo en sucursales.

Cada sucursal debe tener un límite de efectivo específico. Para calcularlo se pueden considerar los siguientes criterios:

a) Ubicación geográfica.
b) Nicho de mercado.
c) Tipo de sucursales.
d) Nivel de Riesgo.

El efectivo existente en las sucursales deberá permanecer protegido con los diversos dispositivos de seguridad física o electrónica que se tengan instalados.

2.1.1. Para definir el límite de existencia, es indispensable que la solicitud haya sido formulada mediante oficio dirigido al titular de la Dirección de la Unidad Estratégica de Inteligencia, signada por titular de la Dirección de la Red de Sucursales, en donde haya aprobado las cantidades propuestas y calificado previamente como razonables, con base en el historial operativo de cada sucursal. La respuesta será emitida por el titular de la Dirección de la Unidad Estratégica de Inteligencia en un lapso no mayor a los 20 días hábiles, a partir de que la recepción de la solicitud contenga la documentación completa.

REVISADO - 9 DIC. 2022

Documentación que se deberá integrar a la solicitud:

a) Oficio solicitud.
b) Listado de sucursales con el límite actual y el monto propuesto.
c) Formato de medidas de seguridad actualizado (TCM-9000-F09-22).
d) Documentos que acrediten la gestión ante las autoridades de seguridad pública, respecto a la vigilancia policial durante las 24 horas.
e) En su caso, evidencia que permita confirmar la vigilancia policial.

Definido el límite máximo de efectivo que debe existir en las sucursales, estas deberán respetarlo invariablemente, concentrando sus excedentes a través de los diversos mecanismos establecidos para tal fin (a través de la empresa especializada de traslado de valores o por medio del procedimiento para el traslado de valores por conducto personal en cualquiera de sus modalidades).

Si por causas ajenas no se puede cumplir con las medidas antes señaladas, los recursos excedentes se depositarán en la caja fuerte de TELECOMM o en su caso, de la compañía trasladadora de valores.

2.2 Límite de efectivo en ventanillas de servicio.

El lugar que resulta más atractivo para cometer un asalto a las sucursales es la línea de ventanillas de servicios. Por ello, la implementación de estrategias de seguridad complementarias a la seguridad física y electrónica con que cuenta permite tener un mayor control sobre los factores de riesgo. El límite de efectivo fijado para las ventanillas de servicio debe respetarse invariablemente, por lo que la persona a cargo de la sucursal debe solicitar al personal de cajas que realice oportunamente la concentración de los excedentes registrados en sus ventanillas, en la caja de valores tantas veces como sea necesario durante su jornada de trabajo.

Para verificar el cumplimiento de la observación anterior, se deberán conservar los registros de las concentraciones que cada caja realiza, cada vez que las existencias hayan superado el límite establecido. Asimismo, para efectos de cumplimiento, se deberán referenciar los métodos establecidos para fijar los límites de efectivo e incluirlos en el punto respectivo y deberá contar con un documento que especifique sus límites asignados, para lo cual las Gerencias Regionales y/o Estatales deberán determinar el monto autorizado.

Si al final de sus operaciones las sucursales rebasan los límites de existencia autorizados, deberán informar a través de correo electrónico a sus Gerencias Regionales y o Estatales para que estas a su vez den aviso a la Subdirección de Seguridad, Investigación y Sistemas de Protección, dependiente de la Dirección de la Unidad Estratégica de Inteligencia sobre dicha situación, dentro de los horarios establecidos para efectos de su inmediata vigilancia por el Centro Nacional de Monitoreo, dependiente de la Gerencia de Monitoreo y Videovigilancia.

La entrega-recepción de remesas de efectivo la efectuará el personal de una compañía trasladadora de valores, siempre y cuando cuente con la capacidad específica para desarrollar dicha actividad, el equipamiento de protección individual adecuado, incluyendo permiso de portación de armas de fuego, transporte blindado y custodio de acompañamiento o de la empresa de transportación de efectivo previamente contratada.

REVISADO - 9 DIC. 2022

Las Gerencias Regionales y/o Estatales deberán considerar que será primordial contar con elementos de seguridad pública, especialmente los días de quincena para que sean asignados a las sucursales de mayor recaudación.

2.3 Procedimiento para detectar faltantes de efectivo en caja.

Para lograr una identificación plena de un acto que se pueda calificar como faltante de efectivo en caja, el Organismo deberá contar con los medios y procedimientos internos, que estarán referenciados puntualmente en el Manual de Procedimientos para la Práctica de Supervisiones Operativas a Sucursales, controlar y auditar en forma sorpresiva o programada las actividades del personal e identificar desviaciones que al ser investigadas y analizadas proporcionen los elementos necesarios para imputar una conducta ilícita por parte del personal.

2.3.1 Para los casos, en que la Gerencia Estatal y/o Regional, a través de la Coordinación Financiera detecte inconsistencias en el flujo de efectivo de las sucursales y por tal motivo, instruya una Supervisión Operativa Especifica o Integral, se deberá dar aviso inmediato a la Dirección de la Unidad Estratégica de Inteligencia y a la Subdirección de Seguridad, Investigación y Sistemas de Protección, así como proporcionar vía telefónica y mediante correo electrónico, el detalle, además de la evidencia documental del hallazgo que originó la supervisión.

2.3.2 La Dirección de la Unidad Estratégica de Inteligencia, en coordinación con la Gerencia Regional y/o Estatal, a través del personal habilitado para llevar a cabo la Supervisión Operativa Especifica o Integral, establecerán una línea de investigación, con objeto de determinar los elementos suficientes en las actas circunstanciadas de hechos y administrativas, que permitan acreditar una conducta grave del personal.

2.3.3 El Coordinador de Supervisión o Supervisor habilitado, al detectar y comprobar la existencia de una faltante en caja simultáneamente, a la integración de la documentación, deberá informar mediante correo electrónico de manera inmediata a la Gerencia Regional o Estatal, la Dirección de la Unidad Estratégica de Inteligencia y la Subdirección de Seguridad, Investigación y Sistemas de Protección y a la Dirección de Asuntos Jurídicos, anexando la documentación que se haya generado hasta el momento.

2.3.4 La Gerencia Regional o Estatal, deberá remitir por correo electrónico, de manera simultánea y dentro de las 24 horas posteriores a la implementación de las actas, a la Dirección de la Red de Sucursales, Dirección de Recursos Humanos, Dirección de Asuntos Jurídicos y Dirección de la Unidad Estratégica de Inteligencia, copia electrónica de la totalidad de la documentación generada.

2.3.5 La Gerencia Regional o Estatal, deberá remitir a la Dirección de la Unidad Estratégica de Inteligencia, la dictaminación emitida por la Dirección de Recursos Humanos y/o la Dirección de Asuntos Jurídicos. Además, deberá informar, respecto al seguimiento del procedimiento y actualización del estatus de la denuncia instrumentada al empleado, así mismo, a través de los medios institucionales disponibles, deberá remitir la documentación que se haya generado al respecto.

2.3.6 La Gerencia Regional y/o Estatal, será la responsable de remitir a la Dirección de la Unidad Estratégica y a la Subdirección de Seguridad, Investigación y Sistemas de Protección, la totalidad de las documentales que integran el expediente de cada uno de los faltantes detectados en la red de sucursales, en los términos del numeral 3.6. del Capítulo VII, del presente documento.

REVISADO - 9 DIC. 2022

3. AUTORIZACIÓN DE PERNOCTAS.

Con relación a los avisos de pernocta de recursos excedentes de operaciones diarias y que son considerados como urgentes, es importante que se tome en cuenta que éstos únicamente procederán cuando exista una verdadera causa de fuerza mayor que la origine.

3.1. MOTIVOS QUE JUSTIFICAN LA PERNOCTA DE RECURSOS

a) Que la empresa Trasladadora de Valores no se haya presentado a realizar la recolección de los recursos, habiendo sido oportunamente solicitada por la Gerencia Estatal.

b) Que se hayan tenido ingresos de efectivo minutos antes de concluir el servicio de la sucursal y se pueda acreditar documentalmente.

c) Que durante la operación del día se hayan obtenido ingresos superiores al límite establecido y la sucursal se encuentre ubicada en zonas de difícil acceso para la empresa trasladadora de valores y que tampoco haya instituciones financieras para concentrar los recursos por lo menos en 50 km a la redonda.

d) Que la sucursal se encuentre dentro de algún programa de ahorro en el esquema de Traslado de Valores y que además cuenten con las medidas suficientes de seguridad y protección. Con relación al programa de ahorro de referencia, éste deberá ser ordenado mediante oficio signado por el titular de la Dirección de la Red de Sucursales, actualizado anualmente y remitido vía correo electrónico a la DUEI con el listado de sucursales en archivo Excel.

e) Circunstancias imprevistas de carácter sociorganizativo, meteorológico, energético, etc.

En todos los supuestos, se deberá acreditar documentalmente cada uno de los argumentos que se exponga al momento de formular la solicitud, además de integrar a su petición, la gestión del apoyo policial ante las autoridades de seguridad pública y los formatos de medidas de seguridad.

Las sucursales cuyas operaciones concluyan a las 15:00 horas, las peticiones deberán formularse vía correo electrónico a la Subdirección de Seguridad, Investigación y Sistemas de Protección, dependiente de la Dirección de la Unidad Estratégica de Inteligencia antes de las 16:00 horas, a fin de que en caso de negarse la pernocta a alguna por falta de medidas de seguridad, se cuente con tiempo para trasladar los recursos a una sucursal cercana que sí cuente con éstas o se tome alguna otra opción, en estos casos la Gerencia Estatal solicitante deberá enviar debidamente requisitado el formato de medidas de seguridad TCM-9000-F09-22 para su análisis y exponer detalladamente los motivos que originen los excedentes de recursos.

En el caso de las sucursales que laboran después de éste horario pero antes de las 19:00 horas, únicamente deberán dar aviso de ésta situación enviando a la Subdirección de Seguridad, Investigación y Sistemas de Protección, dependiente de la Dirección de la Unidad Estratégica de Inteligencia la relación de las sucursales incluyendo las cantidades aproximadas que se quedarán durante la noche, cuyos avisos se harán con límite hasta las 17:00 horas, debiendo detallar la causa que dio origen a dichos excedentes con objeto de que, de inmediato se dé aviso al Centro Nacional de Monitoreo para que de manera prioritaria enfoque su atención a estas, apegándose siempre al mencionado formato para efectos de seguridad.

REVISADO - 9 DIC. 2022

Finalmente, las sucursales que laboran después de las 19:00 horas, o durante sábado y domingo, independientemente de que formulen su aviso a la Dirección de la Unidad Estratégica de Inteligencia, sin considerar horario alguno, deberán marcar copia en el correo electrónico a la Gerencia de Monitoreo y Videovigilancia.

Y en caso de extrema urgencia, además del aviso anterior, hacerlo del conocimiento a la Gerencia de Monitoreo y Videovigilancia a los números telefónicos 5510350248 y 55 50 90 11 00 Ext. 4244, 4247, 4249 y 4262, a fin de que su personal esté en posibilidad de poner atención a dichas sucursales durante el horario nocturno y de fines de semana, no se omite manifestar que siempre deberán apegarse al contenido de su formato de medidas de seguridad TCM-9000-F09-22.

De no acatar las indicaciones anteriores, las sucursales que pernocten con recursos se tendrán por no autorizadas y/o con omisión de aviso y para el desafortunado caso de ser objeto de algún evento delictivo, será responsabilidad única y exclusiva de la Gerencia Estatal de su adscripción.

En la inteligencia de que todas las peticiones y avisos deberán formularse vía correo electrónico directamente a la Subdirección de Seguridad, Investigación y Sistemas de Protección con copia al titular de la Dirección de la Unidad Estratégica de Inteligencia a la siguiente cuenta de correo electrónico:

pernoctas.duei@telecomm.gob.mx

4. TRASLADO DE VALORES.

La actividad de traslado de valores implica un alto riesgo, por lo que, para evitar su agravamiento, sólo se deberá llevar a cabo con personal de las Instituciones de Seguridad Pública o Fuerzas Armadas; especialmente cuando se trate de la ejecución de programas sociales y la empresa trasladadora cuente con los requisitos de seguridad para operar.

4.1 Traslado de valores por conducto personal.

El traslado de valores por conducto personal tiene como principales objetivos, disminuir los costos generados de la contratación de los servicios ofrecidos por las Empresas Trasladadoras de Valores (ETV) y que permite realizar oportunamente la concentración o resguardo de fondos, para que las sucursales de las Gerencias Regionales y Estatales cuenten con el flujo de efectivo necesario para su operatividad.

A continuación, se mencionan los lineamientos que deberán ser observados por las Gerencias Regionales, Estatales y sucursales:

4.1.1 Previo análisis de los factores de riesgo, la Dirección de la Unidad Estratégica de Inteligencia determinará los montos mínimos y máximos a trasladarse por conducto personal, en sus diferentes modalidades (de sucursal de TELECOMM a sucursal bancaria; de sucursal bancaria a sucursal de TELECOMM; de sucursal de TELECOMM a sucursal de TELECOMM y a través de Centros de Distribución y Recaudación).

4.1.2 Cuando la persona a cargo de la sucursal cuente con autorización para trasladar fondos por conducto personal, y lleve a cabo dicha actividad, invariablemente deberá contar con el apoyo policiaco, federal, estatal, local o de aquel que rija en las comunidades en donde se encuentren las sucursales (policía rural, ayuntamientos, comisariatos, etc.).

REVISADO - 9 DIC. 2022

4.1.3 En el caso de que por alguna circunstancia no se pueda obtener el apoyo policiaco, la Gerencia Regional o Estatal podrá autorizar a algún empleado, para que en compañía de la persona a cargo de la sucursal pueda realizar el traslado por conducto personal. Las gerencias, serán las responsables en todo momento de verificar la ejecución de las circunstancias y de las medidas de seguridad establecidas en los numerales 4.1.4, 4.1.5. y 4.1.6.

4.1.4 La Subdirección de Seguridad, Investigación y Sistemas de Protección, observará que los traslados de valores por conducto personal se manejen con los siguientes montos:

a) El traslado podrá realizarlo el empleado de TELECOMM autorizado hasta por $30,000.00 si no se cuenta con seguridad municipal, estatal o federal; siempre y cuando se haga acompañar de otro empleado de la sucursal o Gerencia.

b) Cuando la sucursal de TELECOMM y la sucursal bancaria se encuentren en el mismo inmueble, el personal autorizado podrá efectuar los traslados de valores hasta por un monto de $50,000.00, siempre y cuando se haga acompañar de otro empleado autorizado por la Gerencia.

c) En sucursales multipersonales, el personal autorizado para el traslado de valores podrá realizarlo a las sucursales bancarias tantas veces como sea necesario durante el día, considerando las condiciones establecidas y la continuidad de operaciones en la sucursal, siempre y cuando lo hayan establecido en su solicitud inicial.

4.1.5 El personal autorizado para el traslado de valores, bajo ninguna circunstancia deberá hacerlo con montos mayores a los $50,000, a efecto de no generar un riesgo innecesario para su integridad física, la del personal de TELECOMM que lo acompañe, la seguridad pública y el Patrimonio del Organismo.

Excepcionalmente, la Dirección de la Unidad Estratégica de Inteligencia autorizará trasladar cantidades superiores a las autorizadas, siempre y cuando existan suficientes condiciones de seguridad que permitan llevar a cabo el procedimiento que nos ocupa.

4.1.6 La persona a cargo de la sucursal establecerá diferentes rutas y horarios para llevar a cabo el traslado de valores, a efecto de evitar que se presenten patrones de conducta habitual que permitan a los delincuentes detectar el modo de operación del personal autorizado para trasladar recursos económicos.

4.1.7 Para el caso de aquellas sucursales de carácter unipersonal, que deseen integrarse al esquema de traslado de valores por conducto personal, las Gerencias Regionales o Estatales, serán las responsables de realizar las gestiones necesarias con la finalidad de agotar los procedimientos señalados en los numerales 4.1.2 o 4.1.3 que permitan realizar el traslado de valores de manera segura. Todas las actuaciones realizadas deberán quedar debidamente documentadas.

Excepcionalmente y una vez se hayan agotados los procedimientos descritos en el párrafo anterior sin que se haya obtenido una respuesta favorable por parte de las autoridades, las Gerencias Regionales o Estatales podrán solicitar la opinión por escrito a la DUEI sobre la pertinencia de realizar el traslado de valores por conducto personal.

REVISADO - 9 DIC. 2022

En el escrito de solicitud, las gerencias deberán describir las circunstancias especificas de la localidad y de los factores de riesgo en los que se pretende realizar el traslado tales como: Lugar, distancia, tiempo, medio de transporte, tipo de vialidad, monto a trasladar, horarios, entre otros datos que se consideren relevantes. Es necesario que la solicitud se acompañe del formato de medidas de seguridad TCM-9000-F09-22, las documentales en las que se acredite que se realizaron las gestiones suficientes ante las autoridades y tuvieron una respuesta negativa.

La Dirección de la Unidad Estratégica de Inteligencia emitirá su opinión y las recomendaciones pertinentes en aras de salvaguardar la integridad física de los empleados y los recursos económicos del organismo.

4.1.8 Una vez emitida la opinión de la DUEI, si esta es en sentido afirmativo, las Gerencias Regionales y/o Estatales asumiendo la pertinencia de hacerlo, y verificando que existan las condiciones de seguridad y medios disponibles, podrán autorizar al traslado de valores por conducto personal.

4.1.9. El personal de sucursales unipersonales autorizado para realizar el traslado de valores bajo las condiciones señaladas en el numeral 4.1.7, bajo ninguna circunstancia deberá trasladar montos superiores a los $30,000, a efecto de no generar un riesgo innecesario para su integridad física, la seguridad pública y el patrimonio del Organismo.

4.2 Procesos de coordinación operativa entre la Dirección de la Unidad Estratégica de Inteligencia y las Gerencias Regionales y/o Estatales.

4.2.1 La Dirección de la Unidad Estratégica de Inteligencia determinará qué sucursales estarán autorizadas para realizar el traslado de valores, previo análisis de los elementos de seguridad de cada una de las sucursales propuestas previo análisis de los factores de riesgo.

4.2.2 Los titulares de las Gerencias Regionales y/o Estatales que soliciten autorización para incorporar sucursales al esquema, deberán remitir su solicitud a través de un oficio firmado por el titular de la Gerencia Estatal vía correo electrónico al titular de la Dirección de la Unidad Estratégica de Inteligencia, adjuntando el formato de medidas de seguridad TCM-9000-F09-22 establecido y la respuesta a la petición será enviada en breve siempre y cuando se remita la información necesaria y completa.

4.2.3 El titular de la Dirección de la Unidad Estratégica de Inteligencia, a través del titular de la Subdirección de Seguridad, Investigación y Sistemas de Protección, emitirá los montos mínimos y máximos que podrán ser trasladados por conducto personal, atendiendo a los elementos de seguridad con que cuenten las sucursales propuestas.

4.2.4 La recepción y envío de efectivo o valores deberá efectuarse en áreas de acceso restringido y por personal autorizado por la sucursal, conforme a procedimientos que eviten su exposición a riesgos.

4.2.5 Los titulares de las Gerencias Regionales y Estatales y la persona a cargo de la sucursal solicitarán el apoyo de seguridad a los cuerpos de seguridad pública, agotando los tres niveles de gobierno (Federal, Estatal y Municipal) así mismo, supervisarán su presencia con la finalidad de que se permita su oportuna intervención en caso necesario.

4.2.6 La persona a cargo de la sucursal solicitará ante la autoridad Municipal o Local el apoyo del personal de seguridad para el Traslado de Valores de la sucursal hacia la sucursal bancaria.

4.2.7 El titular de la Gerencia Regional y/o Estatal gestionará, cuando así proceda, ante la autoridad correspondiente de cualquier nivel de gobierno, el apoyo de seguridad para que acompañe al personal que participe en el Traslado de Valores de las sucursales de TELECOMM hacia las sucursales bancarias, informándole a la persona a cargo de la sucursal.

4.2.8 Si las sucursales no cuentan con apoyo de elementos de seguridad pública para el traslado de valores únicamente podrán trasladar como máximo la cantidad de $30,000.00

Si, por el contrario, se acredita mediante la documentación correspondiente que ininterrumpidamente se contará con la colaboración de elementos de seguridad pública durante todo el procedimiento, la Dirección de la Unidad Estratégica de Inteligencia podrá autorizar el traslado de hasta $50,000.00 o más, atendiendo a los factores de seguridad con que se cuente y a las particularidades de cada caso.

4.2.9 Los elementos de seguridad que estén presentes durante el traslado de valores, deberán encontrarse armados.

4.2.10 Se deberá mantener estricto hermetismo en el control de la información en todo lo que respecta al proceso para el ensobrado, traslado y pago de programas sociales, inclusive a empleados que no tengan injerencia en el pago.

4.2.11 Los titulares de las Gerencias Regionales y Estatales deberán enviar al titular de la Dirección de la Unidad Estratégica de Inteligencia, mediante oficio firmado vía correo electrónico la siguiente información y evidencia documental.

a) Plantilla del personal autorizado para participar en el traslado de valores.
b) Cantidades a trasladar.
c) Frecuencia de los traslados (al día, a la semana, etc.)
d) Kilometraje del recorrido
e) Tiempo de recorrido
f) Vehículo a utilizar
g) Documento que garantice el apoyo de seguridad pública.
h) Al término de la ejecución de los traslados informar si se presentaron contratiempos.

4.3 Empresas Trasladadoras de Valores.

4.3.1 Los titulares de las Gerencias Estatales deberán asegurarse de que la empresa que brinda el servicio de traslado de valores, para efectos de control y seguridad cuente con las siguientes medidas básicas indispensables:

a) Catálogo de credenciales con fotografía de los elementos (custodios).
c) Catálogo de firmas de custodios.
d) Vigencia del catálogo de firmas.
e) Reporte de cambio y sustitución de elementos.
f) Especificación de uniformes.
g) Papelería oficial.

REVISADO - 9 DIC. 2022

i) Establecimiento de horarios pertinentes.

4.3.2 El área correspondiente deberá asegurarse que la empresa que preste el servicio de traslado de valores, firme un contrato con este Organismo, en el cual la empresa trasladadora se comprometa alcanzar el máximo grado de eficiencia y optimización en el servicio, que redunde en la plena confiabilidad de la seguridad contratada, además deberá comprometerse expresamente a cubrir con el servicio en el momento en que se requiera.

4.3.3 Es requisito indispensable que el prestador de servicios cuente con equipo de radiocomunicación, sistema de localización satelital para la búsqueda de rutas ante cualquier incidente, vehículos de supervisión exclusivos para las necesidades del servicio que se encuentren blindados, así como exhibir constancia expedida por el proveedor del servicio de blindaje, con la que se acredite el nivel del mismo; equipamiento (chalecos balísticos, uniformes, armas en buen estado), medios de identificación (catálogos de firmas autorizadas, credenciales), procesos de entrenamiento para los usuarios del servicio y si utilizan armas de fuego, la licencia de portación de armas expedido por la Secretaría de la Defensa Nacional.

4.3.4 Deberá tener procedimientos de reclutamiento y selección de personal bien definidos. Esto es, poseer un perfil de puesto para el personal de transporte de valores en el que se determine la edad, peso, estatura, nivel de estudios, antecedentes laborales y habilidades, entre otros.

4.3.5 Durante el servicio, el personal de la trasladadora deberá estar siempre alerta de cualquier extraño que se encuentre en las inmediaciones y que merodee la zona, aplicando las medidas de seguridad respectivas, de acuerdo con los lineamientos de la propia compañía. Asimismo, deberá estar debidamente coordinado y capacitado para detectar y repeler en su caso, cualquier tipo de agresión, incluso para coordinar e implementar de manera inmediata un dispositivo con la intervención de rutas circunvecinas.

4.3.6 El personal de la Trasladadora de valores deberá contar con los siguientes conocimientos y habilidades:

a) Conocer el marco jurídico en el uso y manejo de armamento.
b) Primeros auxilios.
c) Manejo defensivo y evasivo.
d) Prácticas de tiro.
e) Conocimiento de la normatividad en los procesos de recolección y entrega de valores.
f) Curso básico de mecánica.
g) Uso y manejo de sistemas de comunicación.
h) Protección Civil.
i) Planes de reacción en caso de emergencia.
j) Identificación de sospechosos.
k) Trabajo en equipo.

REVISADO - 9 DIC. 2022

CAPÍTULO TERCERO

III. NORMAS DE SEGURIDAD PARA LA EJECUCIÓN DE PROGRAMAS SOCIALES.

1. OBJETIVO.

1.1 Actualizar y mejorar las actividades operativas y de seguridad aplicables durante la ejecución de programas sociales, con especial atención a las zonas de alto riesgo por la presencia de grupos de la delincuencia organizada, gerencias con mayor índice de pérdidas y aquéllas en que se presentan el mayor número de omisiones a las normas establecidas, a fin de establecer las acciones correctivas, modificar, ampliar o establecer nuevas disposiciones de seguridad, que contrarresten las problemáticas que inciden de manera directa en el incremento de pérdidas durante la entrega de estos programas.

2. ANTES DE LA EJECUCIÓN DE PROGRAMAS SOCIALES.

2.1 La Coordinación de Programas Sociales o el área de Seguridad de cada Gerencia Regional y Estatal, deberá coordinarse con la Secretaría del Bienestar para que se agilice la entrega oportuna, de los calendarios de pago de programas sociales, a fin de estar en posibilidad de gestionar con anticipación el resguardo policiaco y estar en condiciones de planear la logística de las rutas de pago, evitando que los servicios sean interrumpidos por cuestiones de jurisdicción policiaca.

2.2 Los titulares de las Gerencias Regionales y Estatales y la persona a cargo de la sucursal sede, en coordinación con la Secretaría del Bienestar y de manera independiente, deberán gestionar ante las instancias de seguridad pública el resguardo policiaco, durante todo el proceso de pago de programas sociales, donde será responsabilidad de los titulares de las Gerentes Regionales y/o Estatales cerciorarse que se materialice el apoyo solicitado antes de realizar cualquier recepción, pernocta y/o traslado de fondos, debiendo reportar por escrito cualquier anomalía a su superior jerárquico, en estricto apego de lo dispuesto en el Manual de Procedimientos para la Entrega de Apoyos Monetarios a Beneficiarios de los Programas Sociales.

El Titular de la Gerencia Regional y/o Estatal en cuanto tenga en su poder los calendarios de pago proporcionados por la Secretaría del Bienestar o a más tardar 48 horas hábiles previas al pago deberá solicitar a la Dirección de la Unidad Estratégica de Inteligencia la recepción o el traslado de remesas para el oportuno pago de los programas sociales, debiendo adjuntar a su solicitud, además del calendario su formato de medidas de seguridad TCM-9000-F09-22 debidamente requisitado.

En caso de que se requiera pernocta de recursos, la Gerencia Regional y/o Estatal al contar con los calendarios de pago, o cuando menos con 48 horas hábiles de anticipación a la fecha en que el pago se haga efectivo, solicitará a la Dirección de la Unidad Estratégica de Inteligencia, la autorización para pernocta, debiendo enviar su calendario en que se definan detalladamente las fechas y las cantidades que pernoctarán, adjuntando su formato de medidas de seguridad TCM-9000-F09-22 con objeto de que la Dirección de la Unidad Estratégica de Inteligencia verifique y determine si las sucursales involucradas reúnen los elementos que garanticen que la pernocta se llevará a cabo de manera segura y se esté en posibilidad de emitir la autorización correspondiente, toda vez que de no contar con las condiciones de seguridad requeridas, la petición será rechazada dando oportunidad a que las inconsistencias se subsanen y se evalúe nuevamente.

REVISADO - 9 DIC. 2022

2.3 Las Gerencias Regionales y/o Estatales deberán supervisar de manera estricta que exista la presencia de las instancias de seguridad pública en los puntos de pago y/o sucursales o sedes convenidas, con la finalidad de garantizar la seguridad de los servidores públicos, de los beneficiarios y de los recursos destinados para el pago de programas sociales.

2.4 El titular de la Gerencia Regional y/o Estatal y las personas a cargo de las sucursales sedes, deberán establecer y fomentar contacto con las autoridades de seguridad pública de los tres niveles de gobierno (Federal, Estatal y Municipal), a fin de garantizar que se brinde el servicio con elementos suficientes y debidamente armados, para el resguardo de los valores destinados al pago de los programas sociales en estricto apego a lo dispuesto en el Manual de Procedimientos para la Entrega de Apoyos Monetarios a Beneficiarios de los Programas Sociales.

2.5 El titular de la Gerencia Regional y/o Estatal deberá solicitar a la Dirección de la Unidad Estratégica de Inteligencia, mediante oficio firmado por él y remitido vía correo electrónico anexado el formato de medidas de seguridad TCM-9000-F09-22 establecido para poder realizar el traslado de remesas superiores a un $1'000,000.00 y para la pernocta de valores en sucursales, desde el momento en que cuente con el calendario de programas sociales o por lo menos con 48 horas hábiles previas a la fecha de pago con la finalidad de evitar que duerman excedentes de efectivo en sucursales que no reúnan las condiciones mínimas de seguridad. En caso de que sea inevitable la pernocta de los remanentes de programas sociales en las sucursales, se deberá solicitar mediante oficio firmado por el titular de la Gerencia Estatal a la Dirección de la Unidad Estratégica de Inteligencia vía correo electrónico, la autorización para el resguardo del efectivo y resguardar al interior de la caja fuerte y/o cofre de seguridad debidamente cerrada con la combinación corrida, y solicitará oportunamente el apoyo de seguridad a las diversas autoridades de seguridad pública, cerciorándose de que acudan al resguardo de los valores informando por el mismo medio a la Dirección de la Unidad Estratégica de Inteligencia con detalle, la fecha de la pernocta, monto y las razones que le dieron origen.

2.6 La Coordinación de Finanzas o área de seguridad pertenecientes a cada Gerencia Regional y/o Estatal, serán las encargadas de verificar que las empresas trasladadoras de valores entreguen las remesas en los horarios y fechas establecidas de acuerdo con el calendario otorgado por el área de dispersión de fondos.

2.7 Queda estrictamente prohibido a las personas a cargo de las sucursales o pagadores habilitados reciban remesas anticipadas a la fecha programada en el calendario de dispersión por parte de las empresas trasladadoras de valores, salvo previo aviso y autorización de su Gerencias Regionales y/o Estatales.

2.8 Previo al proceso de pago, se recomienda solicitar a las corporaciones de seguridad pública federales, estatales y municipales según corresponda su apoyo, para realizar recorridos de supervisión en los caminos y rutas de traslado a las comunidades beneficiadas, con el objeto de identificar los niveles de riesgo y/o modificar la logística para el pago.

2.9 Cuando por cuestiones de logística y el oportuno pago a sus beneficiarios sea necesario que las remesas pernocten en las sucursales, el titular de la Gerencia Estatal, mediante oficio firmado por él, formulará su solicitud a la Dirección de la Unidad Estratégica de Inteligencia inmediatamente después de contar con los calendarios de pago o cuando menos 48 horas hábiles previas a la fecha de pago a sus beneficiarios, debiendo detallar fechas y cantidades, adjuntando el formato de factores de seguridad, así como la evidencia documental y fotográfica con que se acredite la confirmación de los apoyos de los cuerpos de seguridad pública.

REVISADO - 9 DIC. 2022

3. DURANTE EL PROCESO DE PAGO DE PROGRAMAS SOCIALES.

3.1 La persona a cargo de la sucursal no recibirá remesas de programas sociales, si no cuenta con el debido resguardo policiaco, reportándolo de manera inmediata a la Gerencia Estatal y/o Regional.

3.2 Durante la recepción de remesas destinadas a programas sociales deberá establecerse que a corta distancia de la sucursal, se designe a uno o dos empleados con algún medio de comunicación (celular, radio, etc.) ya sea de la propia sucursal u otros designados por la o el titular de la Gerencia Regional y/o Estatal, quienes fungirán como observadores (hasta la salida de las Brigadas de apoyo) y ante el desarrollo de una acción inusual, avisarán de inmediato a las autoridades correspondientes, con el objeto de frustrar el ilícito o lograr la detención de los delincuentes.

3.3 Identificar ampliamente al personal de la empresa de recolección y traslado de valores, verificando lo siguiente antes de que ingresen a la sucursal:

a) Credencial oficial expedida por el Instituto Nacional Electoral vigente con fotografía de los elementos (custodios), en caso contrario será necesario confirmar la identidad de los empleados de la ETV, vía telefónica con la empresa o Gerencia Regional y/o Estatal.
b) Cotejo contra la fotografía.
c) Cotejo de la firma del custodio(s).
d) Vigencia del catálogo de firmas.
e) Verificación del reporte de cambio y sustitución de elementos.
f) Especificación de uniformes.
g) Verificación de la solicitud de concentración de fondos.
h) Papelería oficial.
i) Establecimiento de horarios pertinentes.

3.4 Identificar ampliamente a los elementos y autoridades de seguridad, que sean designadas para custodia y protección de los valores durante el proceso de ensobrado y pago, requiriendo identificaciones oficiales vigentes.

3.5 En caso de no contar con el apoyo de custodia armada, se deberá suspender el proceso de pago de programas sociales y notificar inmediatamente a la Gerencia Regional y/o Estatal, así como a la Dirección de la Unidad Estratégica de Inteligencia en estricto apego de lo dispuesto en el Manual de Procedimientos para la Entrega de los Apoyos Monetarios a Beneficiarios de los Programas Sociales.

3.6 El administrador o pagador habilitado no recibirá remesas de programas sociales, cuando la empresa trasladadora de valores tenga un retraso mayor a una hora. Como caso excepcional, se podrán recibir las remesas fuera del horario de entrega establecido, siempre y cuando exista previa autorización de la Gerencia Regional y/o Estatal, quien deberá gestionar el apoyo de la policía local o regional y valorar si existen las condiciones necesarias, para ejecutar el pago el mismo día o reprogramarlo por las siguientes causas: que por la distancia al o puntos de pago ya no sea posible concluirlo, que ya no se cuente con apoyo policiaco, o las que se consideren pueden generar riesgo para el personal, los beneficiarios y los recursos.

3.7 El titular de la Gerencia Regional y/o Estatal, la Coordinación de Programas Sociales y/o el área de seguridad de cada Gerencia Regional y/o Estatal, deberá verificar que la brigada de pagadores habilitados previo a su salida y durante toda la ejecución del pago de programas sociales, cuenten con el debido resguardo policiaco (elementos suficientes y armados)

previamente gestionado, para realizar el traslado de los recursos, en caso contrario, comunicarse con las autoridades para solucionar dicha eventualidad y en su defecto gestionar ante otra instancia el apoyo, a fin de evitar en la medida de lo posible la cancelación del pago de programas sociales.

3.8 Durante el proceso del pago en los puntos previamente establecidos, se recomendará a las comunidades beneficiadas, que se encuentren alerta ante cualquier situación anormal que pudiera presentar riesgo, avisando de inmediato a las autoridades municipales, ya sea para reforzar las medidas de seguridad o para suspender el pago.

3.9 Las personas a cargo y/o pagadores habilitados, reportarán a él o la titular de la Gerencia Regional y/o Estatal sobre cualquier contrariedad que se presente al inicio del pago de programas sociales como pueden ser: impuntualidad por parte de la empresa trasladadora de valores en la dotación de los recursos, retraso o ausencia de resguardo policiaco en los puntos de pago o sucursales sede, así como de las condiciones en que se les brindará el resguardo policiaco (escaso número de elementos, armas, número de patrullas asignadas, etc.).

3.10 Tratándose de zonas lejanas o aquéllas consideradas de alto riesgo (ya sea por la presencia de grupos de la delincuencia organizada o por el alto índice de ilícitos) en las que se paguen cifras superiores a $500,000.00, la Gerencia Regional y/o Estatal deberá comisionar por brigada al menos tres pagadores habilitados, a fin de concluir con el proceso de pago en el menor tiempo posible y evitar el exceso de remanentes. En caso de no contar con pagadores, deberá fraccionarse el pago en por lo menos dos días, para minimizar las pérdidas en caso de algún evento delictivo.

En la inteligencia de que se requiere que tratándose de remesas superiores a $300,000.00 informe con la oportunidad debida las medidas que se tomarán para fortalecer e incrementar la seguridad durante los operativos de pago.

3.11 El ensobrado del efectivo se deberá llevar a cabo en horas hábiles, dentro del horario de atención, fuera de la vista al público, con el debido resguardo policiaco, evitando estrictamente el acceso a las zonas protegida y crítica, de empleados que no participen en el procedimiento, así como de cualquier persona ajena al Organismo.

3.12 Para el traslado de dinero a los puntos de pago, deberán utilizarse vehículos oficiales sin logotipo del Organismo.

3.13 El Pagador Habilitado durante el ejercicio de su comisión, deberá resguardar en un lugar seguro los recursos destinados a programas sociales, conducirse con diligencia hacia los beneficiarios y abstenerse de ingerir bebidas alcohólicas o cualquier sustancia tóxica.

3.14 Las Coordinaciones de Programas Sociales, Operación, Supervisión y Finanzas, deberán mantener una comunicación permanente durante todo el operativo de pago de programas sociales, para resolver las contingencias que llegarán a presentarse.

4. AL TÉRMINO DE LA EJECUCIÓN DE PROGRAMAS SOCIALES.

4.1 Concluido el proceso de pago, se deberá garantizar la seguridad de los pagadores y el dinero remanente, por lo que se solicitará que los apoyos de seguridad pública que sean designados para vigilancia, protección y custodia, escolten a los pagadores a su regreso a cada sucursal y hasta que el remanente sea depositado en la caja fuerte y/o cofre de seguridad y debidamente cerrados.

REVISADO - 9 DIC. 2022

4.2 La Coordinación de Finanzas perteneciente a la Gerencia Regional y/o Estatal, deberá monitorear diariamente y de manera constante el flujo de efectivo de las sucursales, a fin de avisar con anticipación y en los horarios establecidos a la Dirección de la Unidad Estratégica de Inteligencia sobre la necesidad de pernocta de remesas o remanentes que ocasionen excedentes de efectivo.

4.3 Una vez concluida la entrega de los recursos, el Pagador Habilitado regresará a la sucursal sede para resguardar en la caja fuerte y/o cofre de seguridad el remanente, por lo que queda prohibido que los recursos pernocten en hoteles, automóviles, domicilios particulares u otros lugares que no se encuentren autorizados por la Dirección de la Unidad Estratégica de Inteligencia y la Dirección de la Red de Sucursales, excepto cuando se garantice resguardo de seguridad pública o cualquier otro cuerpo de seguridad fija en el lugar y se cumplan las condiciones de seguridad establecidas para la pernocta de efectivo.

4.4 En el caso de que los pagadores habilitados regresen a la sucursal sede con un remanente que sumado al efectivo existente en caja, supere los límites de existencia autorizados para la sucursal, la persona a cargo de esta, deberá avisar de inmediato al coordinador financiero, que a su vez informará a su Gerencia Regional y/o Estatal, a fin de que vía correo electrónico y en los horarios establecidos dé aviso a la Dirección de la Unidad Estratégica de Inteligencia para que ese efectivo pernocte en la sucursal, asegurándose de que las autoridades de seguridad pública correspondientes proporcionaran el apoyo requerido.

4.5 Las Gerencias Regionales y Estatales autorizarán a la persona a cargo de la sucursal la apertura de la sucursal fuera de su horario laboral únicamente cuando sea estrictamente necesario, para la recepción de remesas y remanentes de programas sociales con la finalidad de que estos no pernocten fuera.

4.6 El dinero de estos programas nunca deberá permanecer de un día a otro dentro de la sucursal, por lo que se deberá concentrar en el banco a través de las empresas aseguradoras de valores y al siguiente día al inicio de las operaciones, solicitar el servicio para continuar con el proceso, a excepción de que se cuente con la autorización para la pernocta de recursos de la Dirección de la Unidad Estratégica de Inteligencia, siempre y cuando se cumplan con las condiciones mínimas de seguridad física, electrónica y apoyo policiaco permanente o a través de rondines.

REVISADO - 9 DIC. 2022

CAPÍTULO CUARTO

IV. PROGRAMA DE SEGURIDAD Y PROTECCIÓN DE TELECOMM.

La Dirección de la Unidad Estratégica de Inteligencia, como responsable de proponer, implementar y supervisar en coordinación con las Gerencias Regionales y/o Estatales, las políticas, estrategias y programas en materia de seguridad e inteligencia, que garanticen el adecuado funcionamiento del Organismo:

Asimismo, se encargará de establecer las políticas para la información y capacitación al personal en caso de la comisión de un delito conforme a las presentes políticas y a la normatividad aplicable.

1. OBJETIVOS:

1.1 Prevenir la comisión de conductas ilícitas.

1.2 Ofrecer a los trabajadores y público usuario, las mejores condiciones de seguridad y protección mientras permanezcan dentro de las instalaciones del Organismo.

1.3 Promover y consolidar una cultura interna de seguridad y protección, propiciando la colaboración y preparación permanente de los servidores públicos en dichas materias.

1.4 Proteger la información financiera de acuerdo con su importancia y trascendencia, así como resguardar adecuadamente los activos informáticos donde es procesada.

1.5 Resguardar y proteger el efectivo y valores que se depositen en las sucursales, mediante la instalación de los dispositivos físicos apropiados y la aplicación de procedimientos seguros por parte de los trabajadores.

1.6 Establecer procedimientos de manejo y traslado seguro de efectivo.

1.7 Garantizar que los sistemas de seguridad se apliquen y funcionen adecuadamente, a través de programas de mantenimiento preventivo y correctivo.

2. PROCEDIMIENTOS PREVENTIVOS DE SEGURIDAD.

Políticas:

a) Será obligación de la persona a cargo de la sucursal, aplicar las normas de seguridad.
b) En caso de no llevarse a cabo estas medidas, la persona a cargo de la sucursal tiene la obligación de reportarlo a su Gerencia Regional y/o Estatal de manera inmediata.

El procedimiento de seguridad y protección de TELECOMM incluye los siguientes procedimientos:

2.1 Antes y durante la apertura de la sucursal:

2.1.1 Deberá cerciorarse de que no existan personas sospechosas en la cercanía a la sucursal especialmente en vehículos estacionados con personas en el interior. En caso positivo, deberá dar aviso a la autoridad correspondiente, así como a la Gerencia Regional y/o Estatal y abrir la sucursal hasta que exista seguridad total.

2.1.2 Deberá abrirse siempre en presencia del elemento de seguridad y de al menos dos empleados, cuando se trate de sucursales multipersonales.

2.1.3 Antes del inicio de operaciones, el responsable deberá hacer un rondín por el interior de la sucursal, con objeto de detectar posibles intrusiones.

2.1.4 Si al entrar a la sucursal se advierte de algo anormal, como perforaciones en los muros, puertas y ventanas rotas o forzamiento en las puertas, se deberá reportar de inmediato a las autoridades de seguridad pública correspondientes, a la Gerencia Regional y/o Estatal y a la Dirección de la Unidad Estratégica de Inteligencia.

2.1.5 Al ingresar, se procederá a desactivar el sistema de alarma y poner en funcionamiento los sistemas y procedimientos complementarios de seguridad, verificando su correcto funcionamiento.

2.1.6 Previo a la apertura al público, se deberá controlar la puerta de acceso para permitir la entrada sólo al resto de los empleados, mismos que no podrán entrar acompañados de terceras personas y vigilarán que no existan personas sospechosas que puedan introducirse al momento de la apertura de la puerta.

2.1.7 No se permitirá la entrada a la sucursal al personal que se encuentre fuera de su horario de trabajo o que se encuentre de vacaciones o días de descanso.

2.2 Durante el Servicio al Público:

2.2.1 Bajo ningún motivo se permitirá el acceso a personas ajenas al Organismo a las áreas de caja fuerte, recuento de efectivo, administrativa y bodega.

2.2.2 Está prohibido el acceso a la sucursal, a personas que no realicen ninguna actividad para el Organismo (Familiares, amigos, vendedores, etc.)

2.2.3 La persona a cargo de la sucursal deberá dotar únicamente del efectivo autorizado a las cajas de servicio al público, supervisando que los operadores de ventanilla no mantengan el dinero sobre el mostrador, y deberá de proveer de efectivo a los operadores de ventanilla tantas veces como el servicio lo requiera, sin que rebase la cantidad autorizada de existencia en el mostrador.

2.2.4 Conservar dentro de las cajas o cofres de seguridad, el grueso de sus existencias, con las combinaciones corridas y debidamente cerradas.

2.2.5 Las lámparas próximas a la caja fuerte y/o cofre de seguridad, se mantendrán encendidas durante las 24 horas, o deberán colocarse sensores de movimiento conectados a la luminaria para que su vigilancia sea fácil desde cualquier posición exterior.

2.2.6 Revisar que las puertas de acceso a los empleados y del área de cajas, permanezcan perfectamente cerradas con llave, durante todo el horario de servicio y durante el ensobrado o conteo de las remesas destinadas al pago de programas sociales.

2.2.7 Si la sucursal cuenta con cortinas o persianas en puertas y ventanas, estás deberán permanecer cerradas totalmente, con el fin de disminuir la visibilidad al interior, sobre todo de las zonas protegidas y críticas.

REVISADO - 9 DIC. 2022

2.2.8 Mantener permanentemente cerradas con llave o seguro las puertas que conectan al interior de la sucursal con el área de ventanillas de servicios.

2.2.9 En el área de ventanillas está prohibido el uso de objetos distractores como: televisores, DVD, juegos electrónicos, teléfonos celulares, audífonos en oídos para escuchar música, periódicos, revistas, libros, etc.

2.2.10 El personal del área de ventanillas, en todo momento deberá estar atento a sus actividades, para detectar y en su caso evitar cualquier tipo de evento.

2.2.11 Al momento de recibir o entregar la remesa de valores, el administrador deberá solicitar la presencia del elemento de seguridad (si cuenta con servicios de vigilancia), además de haber identificado al custodio representante de la empresa recolectora de valores.

2.2.12 En caso de recepción de remesas, la vigilancia de la sucursal será minuciosa y estricta, principalmente hasta que los pagadores entreguen el efectivo al administrador.

2.3 Antes de salir de la sucursal deberá verificar:

2.3.1 Que la caja fuerte y/o cofre de seguridad o compartimientos de resguardo de valores, puertas de acceso y ventanas, estén perfectamente cerradas.

2.3.2 Que los sensores que están ubicados en el área de cajas se encuentren prendidos o en caso de no tener, encender un foco o lámpara ahorradora de energía, con el objeto de no repercutir en los gastos de operación.

2.3.3 Que no quede ninguna persona y/o empleado dentro de la sucursal. Al salir el último empleado, se cerciorará de que no haya ninguna persona extraña al exterior de la que pudiera representar una amenaza.

2.3.4 Que se encuentren cerradas las puertas, ventanas, etc.

2.3.5 Que las sucursales que cuenten con equipos de seguridad electrónico conectado al Centro Nacional de Monitoreo, permanezcan encendidos durante las 24 horas, procurando realizar pruebas de funcionamiento por lo menos dos veces al mes, previo aviso a la Gerencia de Monitoreo y Videovigilancia de la Dirección de la Unidad Estratégica de Inteligencia, en caso de que los equipos se encuentren inhabilitados o en mal funcionamiento deberán reportarlos a su Gerencia Estatal para que se proporcione el mantenimiento respectivo y sean habilitados a la brevedad.

2.3.6 Que, tras efectuar una inspección visual de los alrededores de la sucursal, verificar que no se encuentran personas sospechosas merodeando la zona, vehículos estacionados con personas en su interior; en el caso de detectar algo anormal, deberá reportarlo a las autoridades o corporaciones de seguridad de la zona, solicitando se realicen patrullajes de supervisión y hacerlo de conocimiento del titular de la Gerencia Regional y/o Estatal.

2.3.7 Queda estrictamente prohibido al personal, pernoctar en las sucursales.

2.4 Al Cierre de la sucursal.

2.4.1 Al término del horario del servicio al público, deberán cerrarse todas las puertas de acceso, y el funcionario designado deberá controlar la salida de aquellos usuarios que aún

REVISADO - 9 DIC. 2022

estén dentro de la sucursal, así como controlar las entradas y salidas del personal, cerrando y asegurando la puerta principal en cada ocasión.

2.4.2 Ninguna persona ajena o servidor público no autorizado, podrá ingresar a la sucursal posteriormente a su cierre.

2.4.3 Se deberá resguardar todo recurso en la caja fuerte y/o cofre de seguridad y cerrarla de inmediato terminadas las labores, por lo que está estrictamente prohibido guardar valores financieros en escritorios, archiveros, etc.

2.4.4 Personal del Organismo, de mantenimiento y/o proveedores que se presenten después del cierre o en horario de labores, pero que por sus funciones tengan que ingresar a las áreas restringidas de la sucursal, deberán ser plenamente identificados mediante la credencial oficial de TELECOMM o en el caso de personal externo con la credencial de la empresa que representan, comprobando que exista una orden escrita y autorizada (oficio de comisión) por el área correspondiente (Gerencia Regional y/o Estatal o Áreas Centrales), misma que deberá validar la autenticidad de emisión del documento a fin de evitar la presentación de documentos apócrifos antes de autorizar el ingreso de estos.

2.5 Apertura de caja fuerte y/o cofre de seguridad.

2.5.1 Se hará una vez que se haya realizado la verificación de que todos los dispositivos de seguridad y protección estén operando en condiciones normales.

2.5.2 Los valores deberán quedar debidamente guardados en la caja fuerte y/o cofre de seguridad, mismas que permanentemente tendrán corrida una de las combinaciones o aplicados los temporizadores de apertura.

2.6 Cierre de caja fuerte y/o cofre de seguridad.

2.6.1 Deberá efectuarse en cuanto se concluyan las operaciones de caja, independientemente de que permanezca personal en la sucursal realizando otras labores.

2.6.2 Al cerrarla en forma definitiva, se deberán aplicar los mecanismos de seguridad de cada dispositivo.

3. PROCEDIMIENTOS DE CONTROL DE DISPOSITIVOS, MECANISMOS, SISTEMAS DE INFORMÁTICA Y DE COMUNICACIÓN Y EQUIPO TÉCNICO DE PROTECCIÓN.

Todos los dispositivos, mecanismos y sistemas de seguridad, deberán estar sujetos a un control estricto, para evitar su uso indebido o abusos por parte de los trabajadores o terceros.

Los controles básicos que se deben aplicar son:

a) Controles a los sistemas de seguridad.
b) Controles para la aplicación de las normas de seguridad.
c) Controles de seguridad física.

REVISADO - 9 DIC. 2022

3.1 Controles a los Sistemas de Seguridad.

3.1.1 Cada sucursal deberá contar con un inventario de los sistemas de seguridad instalados. Las Gerencias Estatales deberán remitir la actualización de dicha información a la Dirección de la Unidad Estratégica de Inteligencia, por lo menos de forma anual y en el formato solicitado.

3.1.2 La operación de los sistemas y equipos de seguridad instalados en cada sucursal, será responsabilidad del personal previamente capacitado y facultado.

3.1.3 El acceso a los controles deberá registrarse en una bitácora con acceso sólo al funcionario designado.

3.1.4 Deberá manejarse un registro de asignación y cambio periódico de claves para la operación de los sistemas.

3.1.5 El reporte de fallas deberá estar autorizado por el funcionario facultado.

3.1.6 El mantenimiento, instalación, cambio o reubicación de los equipos electrónicos de seguridad, deberá contar con una orden de servicio que será autorizada por la Dirección de la Unidad Estratégica de Inteligencia y la Dirección de la Red de Sucursales. Para lo cual, el programa deberá ser enviado anualmente en el primer mes de cada año a la Dirección de la Unidad Estratégica de Inteligencia.

3.1.7 El personal facultado deberá revisar diariamente que los sistemas y equipos de seguridad instalados se encuentren funcionando correctamente. Para ello deberán realizarse las siguientes verificaciones:

a) Observar que el estado físico de los diversos dispositivos sea normal y que no presenten signos evidentes de deterioro, alteración o vandalismo.
b) Verificar que las cámaras del sistema de video grabación de imágenes no se encuentren obstruidas o fuera de su posición original y que se encuentren encendidas.
c) Revisar que los paneles de control de los sistemas de alarma y de video grabación de imágenes se encuentren encendidos.
d) Realizar una prueba de funcionamiento del sistema de video grabación de imágenes.

3.1.8 Las pruebas de funcionamiento de los diferentes sistemas de seguridad deberán registrarse en una bitácora, donde contenga el nombre de la sucursal, nombre de la persona a cargo de la sucursal, fecha de realización, por quien fue realizado, las condiciones en que se encontraron, así como las recomendaciones pertinentes. Los sistemas que deberán ser inspeccionados son:

a) Transfer o mecanismos de retardo.
b) Sistemas de informática y de comunicación.
c) Sistemas de grabación de imágenes y monitoreo.
d) Central local de alarmas.
e) Equipo técnico de protección.
f) Mecanismos de seguridad.
g) Encristalamiento de ventanillas.

REVISADO - 9 DIC. 2022

3.1.9 La capacitación sobre el uso y operación de los sistemas y equipos de seguridad instalados, deberá ser proporcionada por personal de la Dirección de la Unidad Estratégica de Inteligencia en coordinación con la Dirección de Recursos Humanos.

3.2 Controles para la aplicación de las normas de seguridad.

3.2.1 Los titulares de las Gerencias Estatales y/o Regionales serán los encargados de designar a la persona a cargo de la sucursal, para asegurar la correcta aplicación de las normas de seguridad y protección por parte del personal, registrando esta designación mediante la firma de un acta en la que se acepte dicha responsabilidad.

En caso de que la persona a cargo de la sucursal se ausente por alguna situación (personal o laboral), deberá elaborar un Acta de Entrega-Recepción de la sucursal, donde se designe al responsable y se realicen los cambios de contraseñas de ingreso al SIGITEL y se cambien las combinaciones de la caja fuerte y/o cofre de seguridad, así como la entrega de las llaves de la sucursal y el aviso de término de la Entrega-Recepción. Del mismo modo, la persona que quede a cargo deberá realizar el mismo procedimiento al momento de entregar nuevamente la sucursal, en apego a lo establecido en el Manual de Procedimientos para la Operación de Sucursales.

3.2.2 A través de los diferentes medios de control descritos, el funcionario responsable deberá demostrar el cumplimiento de dichas normas.

3.2.3 La persona a cargo de la sucursal, deberá dar seguimiento a los procesos, sistemas y controles operativos para la prevención y detección de irregularidades, en la realización de operaciones y en el manejo de los valores.

3.2.4 La prevención y detección de irregularidades en la realización de operaciones y en el manejo de los valores, se debe realizar a través de los siguientes medios como parte de las estrategias de seguridad:

a) Medios verificables de prevención y detección de irregularidades. Arqueos de caja, detección de faltantes y sobrantes.
b) Verificación de firmas para asegurar la autenticidad del girador. Cajero de ventanilla y supervisor.
c) Medios verificables de prevención y detección de irregularidades. Objetivo del medio responsable y pago, dentro de facultades.
d) Corresponsabilidad de pagos. Cajero de ventanilla, supervisor y nivel superior.
e) Verificación de documentos, asegurar su literalidad. Cajero de ventanilla y supervisor.
f) Verificación de billetes, asegurar su autenticidad. Cajero de ventanilla, supervisor y cajero principal.
g) Verificación de resguardo y concentración de efectivo. Mantener límites máximos establecidos.
h) En las sucursales abiertas al público en general, los elementos de control de acceso se concentran en el personal y en la prohibición de ingreso del público fuera de las horas autorizadas para su atención.

3.3. Controles de Seguridad Física.

El establecimiento de controles para la seguridad física, tienen el objetivo de proteger toda la propiedad dentro de los límites de las instalaciones, así como salvaguardar la seguridad de los empleados y otras personas que están dentro del mismo.

Los principales controles que se deberán establecer son:

a) Identificación de empleados con credencial de TELECOMM.
b) Registro escrito de entradas y salidas del personal a las instalaciones.
c) Ingreso y salida libre, en horarios autorizados.
d) Verificación del retiro del personal.
e) Salida controlada al cierre de las operaciones.
f) Control de asistencia en horas y días inhábiles (previa autorización).
g) Control de público cuya permanencia interna no esté justificada.
h) Control de vendedores, personas en situación de calle, promotores y personas en estado inconveniente.
i) Al ingreso de los usuarios a las sucursales que se encuentren hablando por celular, porten gorras, sombreros, cascos de motociclista, sudadera con gorro, lentes oscuros o cualquier prenda que cubra parcial o enteramente su rostro, deberá indicárseles que está prohibido realizar dichas prácticas dentro de las instalaciones.
j) En caso de observar, en los alrededores de las sucursales, personas sospechosas, cerca de las inmediaciones, deberá reportarse de manera oportuna a las autoridades correspondientes y al titular de la Gerencia Regional y/o Estatal.

4. PROGRAMA DE REGULARIZACIÓN DE SUCURSALES EN MEDIDAS BÁSICAS DE SEGURIDAD.

Las Gerencias Regionales y/o Estatales deberán elaborar de manera anual un programa para la implementación de medidas básicas de seguridad, priorizando las sucursales que requieran de atención inmediata.

El programa deberá ser factible de alcanzar con los recursos disponibles, con la estrategia adoptada y dentro de los plazos que se programen, asimismo deberá ser supervisado y actualizado constantemente.

4.1 Objetivo.

Lograr de manera gradual que todas las sucursales cuenten con las medidas básicas de seguridad, con el objeto de asegurar la integridad física de empleados, usuarios, bienes y valores del Organismo, apegándose a los lineamientos establecidos en las presentes Políticas de Seguridad.

4.2. Criterios de Aplicación.

4.2.1 Mantener las condiciones de seguridad en las sucursales, evitando circunstancias que pongan en riesgo la integridad física de los empleados, clientes, la operación y el patrimonio institucional.

4.2.2 Incremento en el índice delictivo de acuerdo con información proporcionada por la Dirección de la Unidad Estratégica de Inteligencia a través de la Subdirección Seguridad, Investigación y Sistemas de Protección y Supervisión a nivel entidad, alcaldía o municipio.

4.2.3 Identificación de zonas geográficas que apoyen o favorezcan la implantación.

4.2.4 Nivel de obsolescencia de los equipos electrónicos.

REVISADO - 9 DIC. 2022

4.3. Elementos que se requieren para formular un programa de regularización:

4.3.1 Diagnóstico del problema
El titular de la Gerencia Regional y/o Estatal describirá la problemática detectada, como resultado de la evaluación del formato de medidas de seguridad TCM-9000-F09-22 de las medidas de seguridad que tienen las sucursales de su jurisdicción.

4.3.2 Justificación
Definir cuál es la necesidad de efectuar la regularización y/o mejora a partir del diagnóstico, especificando los beneficios o aportaciones que se esperan obtener para el Organismo.

4.3.3 Objetivo
Indicar como se llevará a cabo su implementación.

4.3.4 Acciones específicas
Serán mencionadas las actividades concretas que se efectuarán para eliminar o controlar las deficiencias, relacionado con el objetivo del programa.

4.3.5 Localización
Son las sucursales que están contempladas para formar parte del programa de regularización emergente durante el año siguiente al de elaboración, donde el titular de la Gerencia Regional y/o Estatal deberá seleccionar las sucursales con la mayor vulnerabilidad e impacto para el Organismo que pongan en riesgo la vida de los empleados y usuarios, por lo que su atención deberá ser inmediata.

4.3.6 Calendarización
Se elaborará un cronograma con las principales actividades que se realizarán, considerando los tiempos programados. Hacer la programación trimestral. Anexo 2.

4.3.7 Recursos humanos
Es el personal interno o externo que se considera apto para realizar los trabajos de mejora.

4.3.8 Recursos materiales.
Son las Instalaciones, materiales y/o equipo necesario.

4.3.9 Recursos financieros.
Es el presupuesto que se estima necesario para efectuar el Programa de Regularización de Sucursales en Medidas Básicas de Seguridad y que es preciso solicitar.

REVISADO - 9 DIC. 2022

CAPÍTULO QUINTO

V. PLAN DE ATENCIÓN A EMERGENCIAS.

Deberá aplicarse siempre ante un evento delictivo, con el conocimiento y supervisión de las Gerencias Regionales y/o Estatales y la Dirección de la Unidad Estratégica de Inteligencia.

1. OBJETIVO.

Conocer y aplicar los planes de emergencia para cada tipo de riesgo.

2. GENERALIDADES.

Una situación de crisis en las sucursales se genera cuando el personal, público usuario y/o activos, están siendo sujetos de una situación imprevista, un evento delictivo en curso o un suceso de la naturaleza o evento socio organizativo que pone en riesgo su seguridad.

En estas condiciones, al aplicarlo permitirá controlar la situación de riesgo, reducir y mitigar su impacto y restablecer la continuidad de sus operaciones en un tiempo razonablemente corto.

3. POLÍTICAS DE ACTUACIÓN EN CASO DE EMERGENCIA.

3.1. EN CASO DE PRESENTARSE LAS SIGUIENTES CONTINGENCIAS.

Los responsables de la sucursal deberán adoptar las siguientes líneas de acción en caso de presentarse estas situaciones:

3.1.1 Al cerrarse y/o bloquearse el sistema informático Sigitel antes del horario establecido.

Cuando se bloquee el sistema asignado a los operadores, podrá realizar el desbloqueo la persona a cargo de la sucursal, a fin de corregir esta situación y continuar con las operaciones normales. Si el cierre es intempestivo y no hay forma de remediarlo, no se encuentra el administrador o la cuenta de la persona a cargo de la sucursal también se encuentra bloqueada, se deberá informar vía telefónica a su Coordinación de Operación de la Red de Sucursales, para que por su conducto sea remediado.

3.1.2 Por cortes de energía eléctrica y el personal tenga que esperar para enviar el MODIFO y cerrar la sucursal.

Cuando se suscite un corte de energía eléctrica y para prevenir que en la confusión malhechores puedan hacer uso de estos incidentes para efectuar un asalto o intrusión y apoderarse de los caudales de dicha sucursal; si aún se encuentra público usuario, deberán invitarlos a salir a causa de la falla, procediendo a cerrar la sucursal y a resguardar los valores monetarios en la caja fuerte y/o cofre de seguridad.

Si la falta del suministro de energía eléctrica se presenta antes de iniciar operaciones, la sucursal no se apertura al público usuario, ni tampoco la caja fuerte y/o cofre de seguridad, en tanto no se restablezca el servicio referido.

REVISADO - 9 DIC. 2022

En ambos casos la persona a cargo de la sucursal deberá reportar de inmediato la anomalía a la Comisión Federal de Electricidad, solicitando se informe la causa y el tiempo estimado que durará esa zona sin energía eléctrica.

Con esta información deberá informar a su Gerencia Regional y/o Estatal y a las Direcciones de la Red de Sucursales y de la Unidad Estratégica de Inteligencia, la situación que prevalece en la sucursal y posteriormente, el momento en que se restablecieron las operaciones.

Si al término de las labores no se resolvió esta situación, el cierre del MODIFO lo deberá realizar la persona a cargo de la sucursal al siguiente día al inicio de labores, en caso de que la falla continúe deberá reportarlo a su Gerencia Regional y/o Estatal para que su Coordinación de Finanzas, realice el cierre por contingencia y una vez restablecida la falla, la persona a cargo de la sucursal deberá cerciorarse que todos los movimientos estén debidamente registrados, confirmando por escrito a su gerencia que los datos son correctos.

Asimismo, es importante mencionar que la Gerencia Regional y/o Estatal, deberá mantener un monitoreo permanente sobre la falla de energía eléctrica en esta sucursal, con el objeto de considerar con oportunidad las medidas de seguridad pertinentes para el resguardo de los valores monetarios, en caso de no restablecerse el servicio, lo deberá notificar a la Dirección de la Unidad Estratégica de Inteligencia.

3.1.3 Por cargas de trabajo principalmente cuando se atiende el pago de programas sociales.

Cuando las sucursales lleven a cabo el pago de programas sociales, la persona a cargo de la sucursal deberá prever las cargas de trabajo y si llegada la hora del cierre de la base de datos del servidor no se concluye con la descarga de la información, deberá avisar a su Gerencia Regional y/o Estatal, a la Dirección de la Red de Sucursales y a la Dirección de la Unidad Estratégica de Inteligencia, para que se puedan tomar las medidas o acciones que correspondan.

3.1.4 Apertura de las sucursales en días y horarios que no laboran; específicamente cuando se realiza la entrega de apoyos de programas sociales.

Esta estrictamente prohibido brindar servicio al público usuario fuera de los horarios y días establecidos por cada sucursal, a menos que se trate de una causa justificada y sin excepción, deberá contar con previa autorización de su Gerencia Regional y/o Estatal. Así también, es necesario se informe de estos cambios a la Dirección de la Unidad Estratégica de Inteligencia, a efecto de supervisar las instalaciones a través del Centro Nacional de Monitoreo.

3.2 EN CASOS DE ASALTO.

En caso de presentarse un asalto, el administrador de la sucursal, personal operativo y elementos de vigilancia, deberán adoptar las siguientes acciones y medidas según corresponda a cada una de sus funciones:

3.2.1 Antes.

REVISADO - 9 DIC. 2022

3.2.1.1 El personal de la sucursal deberá tener el efectivo resguardado adecuadamente en la caja fuerte y/o cofre de seguridad, los cuales deberán estar debidamente cerrada y con la combinación corrida.

3.2.1.2 Todos los dispositivos de alarma deberán estar en adecuadas condiciones de funcionamiento y transmitir las señales necesarias tanto de alarma como de imágenes al ser activadas, mismos que deberán quedar conectados a las centrales de alarma de cuerpos policiacos y al Centro Nacional de Monitoreo.

3.2.1.3 Los dispositivos electrónicos de acceso a las zonas protegidas y críticas, deberán estar en correcto funcionamiento.

3.2.1.4 El personal que atienda público usuario en el área de ventanillas de servicios, estará alerta a detectar cualquier acción, persona o situación que sea considerada sospechosa, reportándola de inmediato a la persona a cargo de la de sucursal.

3.2.1.5 En caso de confirmarse la situación sospechosa, la persona a cargo de la sucursal deberá dar aviso inmediato a la central de policía más cercana, así como a la Dirección de la Unidad Estratégica de Inteligencia.

3.2.1.6 Los operadores de ventanilla deberán respetar los montos máximos autorizados para retener en ventanilla y en caja fuerte, con la finalidad de evitar pérdidas mayores para TELECOMM.

3.2.2 Durante.

3.2.2.1 En todo evento de este tipo la premisa deberá ser la preservación de la vida de los empleados y usuarios, en segundo término, de los bienes y valores que se manejan en cada sucursal.

3.2.2.2 El personal de la sucursal, deberá activar el botón de pánico.

3.2.2.3 Si la sucursal cuenta con alarma conectada al Centro Nacional de Monitoreo y si los delincuentes piden que se desactive, deberán oprimir el "código de amago". Esta clave inhibirá el sonido de la alarma y el aviso de emergencia será recibido en el Centro Nacional de Monitoreo.

3.2.2.4 No intente persuadir al asaltante(s).

3.2.2.5 Se procurará entregar al delincuente la menor cantidad posible de efectivo, tratando de dar los billetes de más baja denominación.

3.2.2.6 El personal que haya presenciado el asalto deberá mantener la calma y asumir una actitud pasiva pero alerta, a efecto de observar los mayores detalles del hecho delictivo, así como de los asaltantes: su aspecto físico, estilo forma de vestir, zapatos, acento de voz, forma de moverse, tics, defectos físicos (cicatrices), tatuajes, características de armas, etc.; de forma tal que sus aportaciones contribuyan a la investigación del ilícito.

3.2.2.7 De ser posible se verificarán las características del transporte utilizado (placas, color, modelo, marca, golpes o abolladuras, dirección en la que arribaron y se evadieron).

REVISADO - 9 DIC. 2022

3.2.3 Después.

3.2.3.1 Una vez que los asaltantes salieron, se deberán cerrar de inmediato las puertas de acceso.

3.2.3.2 Se mantendrán las condiciones intactas que tiene el escenario del delito, para ello deberán protegerse las áreas donde se desarrolló el hecho delictivo, cuidando no tocar el dinero remanente y los objetos con los que tuvieron contacto los asaltantes.

3.2.3.3 Se reportará de inmediato a las autoridades más cercanas de este hecho, siendo estas las estatales o municipales, a efecto de que tomen conocimiento de lo ocurrido, se inicien las averiguaciones correspondientes y se levanten las evidencias existentes.

3.2.3.4 La persona a cargo de la sucursal hará de conocimiento los hechos vía telefónica o por los medios más expeditos a la Gerencia Regional y/o Estatal y a la Dirección de la Red de Sucursales, a la Dirección de la Unidad Estratégica de Inteligencia y a la Dirección de Asuntos Jurídicos, ésta última dará asesoría para que se proceda al levantamiento del acta ante la autoridad correspondiente y se proceda conforme a la normatividad establecida.

3.2.3.5 Si hubiera toma de rehenes en la huida de los delincuentes, deberá reportar la situación a la Dirección de la Unidad Estratégica de Inteligencia para que se determinen los procedimientos necesarios para preservar la vida del personal involucrado.

3.2.3.6 Una vez que los asaltantes salgan, se revisará que no haya personal o público usuario lesionado. Si hubiera personas afectadas, deberá solicitar la presencia de los cuerpos de auxilio médico de emergencia y reportar todos los acontecimientos de inmediato a la Dirección de la Unidad Estratégica de Inteligencia.

3.2.3.7 La persona a cargo de la sucursal junto con el coordinador de supervisión, deberán realizar internamente los arqueos necesarios en cada una de las áreas donde ocurrió el evento delictivo y se deberán documentar todas las incidencias observadas.

3.2.3.8 Por ningún motivo se informará sobre la cantidad de dinero robada al personal ajeno al Organismo y de la cantidad sobrante en las gavetas y caja fuerte hasta que no se hayan realizado los arqueos correspondientes. Se deberá proporcionar Información sólo a personas autorizadas por la Gerencia Regional y/o Estatal.

3.2.3.9 Se verificarán los activos sustraídos y/o dañados, así como los equipos, materiales y documentos faltantes.

3.2.3.10 Se deberá esperar notificación de la Gerencia Regional y/o Estatal para el reinicio de las operaciones.

REVISADO - 9 DIC. 2022

3.2.3.11 La persona a cargo de la sucursal, el personal que presenció el hecho delictivo y la Dirección de Asuntos Jurídicos, deberán cooperar con la investigación del hecho por las autoridades que correspondan.

3.2.3.12 Se deberán proporcionar las facilidades necesarias para que las autoridades, peritos y personal del Organismo realicen investigaciones evitando modificar las condiciones del delito, ocultar o modificar la información o encubrir a personas que pudieran estar involucradas con el delito.

3.2.3.13 Cada Gerencia Regional y/o Estatal formulará y remitirá a la Dirección de la Unidad Estratégica de Inteligencia, al Órgano Interno de Control, a la Dirección de Asuntos Jurídicos, a la Gerencia de Supervisión de Sucursales y a la Unidad de Seguros y Fianzas un informe detallado que responda a las interrogantes: ¿Qué? ¿Quién? ¿Cuándo?, ¿Dónde? y ¿Cómo? acciones que se tomaron, autoridad que intervino, número de acta o averiguación previa, monto de lo sustraído, situación que prevalece en la sucursal y hora de reinicio de actividades. De igual manera deberá notificar de inmediato vía telefónica a la Dirección de la Unidad Estratégica de Inteligencia lo ocurrido de manera sucinta y remitir a más tardar en cinco días hábiles, debidamente requisitado el informe del evento delictivo conforme a los puntos preestablecidos que para tal efecto emita la citada Dirección.

3.3 EN CASOS DE ROBO POR INTRUSIÓN O TENTATIVA DE ROBO POR INTRUSIÓN.

En caso de presentarse un robo por intrusión o una tentativa de robo por intrusión, el administrador de la sucursal, personal operativo y elementos de vigilancia, deberán adoptar las siguientes acciones y medidas según corresponda a cada una de sus funciones:

3.3.1 Antes.

3.3.1.1 El personal de la sucursal deberá tener el efectivo resguardado adecuadamente en la caja fuerte y/o cofre de seguridad, los cuales deberán estar debidamente cerrados y con la combinación corrida.

3.3.1.2 Los operadores de ventanilla deberán respetar los montos máximos autorizados para retener en ventanilla y en caja fuerte, con la finalidad de evitar pérdidas mayores para TELECOMM.

3.3.1.3 Todos los dispositivos electrónicos deberán estar en adecuadas condiciones de funcionamiento y transmitir las señales necesarias tanto de alarma como de imágenes al ser activadas, mismos que deberán quedar conectados al Centro Nacional de Monitoreo o en su caso, a las centrales de alarma de cuerpos policiacos.

3.2.1.4 Los dispositivos electrónicos de acceso a las zonas protegidas y críticas, deberán estar en correcto funcionamiento.

3.3.1.5 El personal operativo, estará alerta a detectar cualquier acción, persona o situación que sea considerada sospechosa, reportándola de inmediato la persona a cargo de la sucursal y este a su vez, deberá dar aviso a la Gerencia Estatal, a las autoridades de seguridad pública y a la DUEI.

REVISADO - 9 DIC. 2022

3.3.1.6 En caso de detectar alguna anomalía o daños en el inmueble, así como de confirmarse la situación sospechosa, la persona a cargo de la sucursal deberá dar aviso inmediato a la central de policía más cercana, a la Dirección de la Unidad Estratégica de Inteligencia y simultáneamente a la Gerencia Estatal.

3.3.2 Durante la detección.

3.3.2.1 En caso de que el personal al arribar a la sucursal detecte indicios de entrada forzada, deberá reportar inmediatamente a la central de policía más cercana, a la Dirección de la Unidad Estratégica de Inteligencia y simultáneamente a su Gerencia Estatal.

3.3.2.2 El personal deberá preservar el lugar, evitando ingresar a la sucursal, tocar o alterar todo aquello que se pueda considerar como indicio, o bien contribuya a la investigación.

3.3.2.3 El personal que haya detectado la intrusión deberá colaborar y proporcionar toda la información necesaria a la Dirección de la Unidad Estratégica de Inteligencia, mediante entrevistas a través de los medios tecnológicos disponibles o de manera personal, con la finalidad de que sus aportaciones contribuyan a la investigación del ilícito.

3.3.3 Después.

3.3.3.1 Se mantendrán las condiciones intactas que tiene el escenario del delito, para ello deberán protegerse las áreas donde se desarrolló el hecho delictivo, cuidando no tocar el dinero remanente y los objetos con los que tuvieron contacto los asaltantes.

3.3.3.2 Se reportará de inmediato el arribo de las autoridades, a efecto de que se informe el estatus de la ejecución de los peritajes y de las evidencias existentes.

3.3.3.3 La persona a cargo de la sucursal o el trabajador que haya detectado el ilícito, actualizará por lo menos cada 24 horas el estatus de los hechos vía telefónica o por los medios más expeditos a la Gerencia Regional y/o Estatal y a la Dirección de la Red de Sucursales, a la Dirección de la Unidad Estratégica de Inteligencia y a la Dirección de Asuntos Jurídicos, ésta última dará asesoría para que se proceda a la presentación de la denuncia ante la autoridad correspondiente y se proceda conforme a la normatividad establecida.

3.3.3.4 En casos donde se realice una detención por parte de las autoridades, no intentar negociar con los delincuentes o sus representantes.

3.3.3.5 Está estrictamente prohibido el ingreso a la sucursal a personas ajenas al Organismo, con excepción de los cuerpos policiacos.

3.3.3.6 La persona a cargo de la sucursal junto con el coordinador de supervisión, deberán realizar internamente los arqueos necesarios en cada una de las áreas donde ocurrió el evento delictivo y se deberán documentar todas las incidencias observadas.

REVISADO - 9 DIC. 2022

3.3.3.7 Por ningún motivo, se informará a personas ajenas al Organismo sobre la cantidad de dinero robada o la cantidad sobrante en las gavetas y caja fuerte.

3.3.3.8 Una vez cuantificados los daños se informará por escrito el monto de efectivo sustraído, así como los bienes muebles e inmuebles faltantes, dañados o destruidos, incluyendo equipos electrónicos, materiales y /o documentos.

3.3.3.9 Se deberá esperar notificación de la Gerencia Regional y/o Estatal para el reinicio de las operaciones.

3.3.3.10 La persona a cargo de la sucursal, el personal que presenció el hecho delictivo y la Dirección de Asuntos Jurídicos, deberán cooperar con la investigación del hecho por las autoridades que correspondan.

3.3.3.11 Se deberán proporcionar las facilidades necesarias para que las autoridades, peritos y personal del Organismo realicen investigaciones evitando modificar las condiciones del delito, ocultar o modificar la información o encubrir a personas que pudieran estar involucradas.

3.3.3.12 Cada Gerencia Regional y/o Estatal formulará y remitirá a la Dirección de la Unidad Estratégica de Inteligencia, a la Dirección de Asuntos Jurídicos, a la Gerencia de Supervisión de Sucursales y a la Unidad de Seguros y Fianzas un informe detallado que responda a las interrogantes: ¿Qué? ¿Quién? ¿Cuándo?, ¿Dónde? y ¿Cómo? acciones que se tomaron, autoridad que intervino, número de acta o averiguación previa, monto de lo sustraído, situación que prevalece en la sucursal y hora de reinicio de actividades. De igual manera deberá notificar de inmediato vía telefónica a la Dirección de la Unidad Estratégica de Inteligencia lo ocurrido de manera sucinta y remitir a más tardar en cinco días hábiles, debidamente requisitado el informe del evento delictivo conforme a los puntos preestablecidos que para tal efecto emita la citada Dirección.

3.4 EN CASO DE ACTOS FRAUDULENTOS.

3.4.1 Antes

3.4.1.1 El supervisor, la persona a cargo de la sucursal y personal operativo, deberán conocer a detalle las acciones a seguir en este caso.

3.4.1.2 Conservar la calma y actuar de manera normal, sin tratar de hacer movimientos que alerten al defraudador.

3.4.2 Durante

3.4.2.1 El personal que identifique la posibilidad de una situación de estas en su ventanilla de servicio, deberá indicar al posible defraudador que le permita completar la operación solicitada, retirándose de la caja y notificando discretamente la situación a su jefe inmediato e informándole de los documentos que están generando la duda.

REVISADO - 9 DIC. 2022

3.4.2.2 El supervisor deberá analizar los documentos y/o transacciones, e informar los hechos a la persona a cargo de la sucursal, quien analizará y determinará si se requiere la intervención de las autoridades activando la señal de alarma.

3.4.2.3 Una vez activada la señal de alarma, en cuanto sea posible se deberá confirmar telefónicamente el motivo de la alerta a la Gerencia de Monitoreo y Videovigilancia.

3.4.2.4 Si la persona a cargo de la sucursal considera que hay elementos suficientes, deberá solicitar la presencia de las autoridades y de la Dirección de la Unidad Estratégica de Inteligencia y retener los documentos en cuestión.

3.4.2.5 Se intentará entretener a la persona involucrada para que permanezca en la sucursal hasta que llegue la ayuda externa.

3.4.2.6 Al arribar el apoyo, la persona a cargo de la sucursal deberá entregarle los documentos y señalar a la persona involucrada si aún se encuentra.

3.3.3 Después

3.4.3.1 Deberán documentarse los actos fraudulentos, reuniendo todos los elementos, documentos y observaciones que puedan contribuir a la investigación del caso y al deslinde de responsabilidades del personal que sufrió la tentativa.

3.4.3.2 La persona a cargo de la sucursal deberá realizar un informe de lo sucedido y entregarlo a la Dirección de la Unidad Estratégica de Inteligencia, en un plazo que no excederá de un día hábil posterior a la comisión del ilícito.

3.4.3.3 La persona a cargo de la sucursal y el personal que fue testigo del hecho delictivo, deberán colaborar con las autoridades correspondientes respecto de la investigación del hecho.

3.4.3.4 En el caso de que exista actos que deriven en faltantes de efectivo por parte de personal de TELECOMM, la Coordinación de Operación de la Red de Sucursales de la Gerencia Regional y/o Estatal donde se presente tal circunstancia, realizará la documentación contable del agravio al Organismo, en conjunto con la Dirección de la Red de Sucursales, quien además es responsable de emitir a todas las sucursales a nivel nacional las políticas y disposiciones que norman la operación, como el manejo de log-in passwords y la seguridad de su uso para tener acceso al sistema Sigitel en línea.

3.4.3.5 De inmediato se reportará el evento a la Coordinación Jurídica de la Gerencia Estatal, quien dará aviso a la Dirección de la Unidad Estratégica de Inteligencia, a la Dirección de la Red de Sucursales, a la Dirección de Administración, a la Dirección de Recursos Humanos, al Órgano Interno de Control y a la Dirección de Asuntos Jurídicos para que de inmediato actúen en el ámbito de su competencia.

3.5 EN CASO DE EXTORSIÓN.

3.5.1 Antes.

3.5.1.1 Tener a la mano los números de emergencia.

REVISADO - 9 DIC. 2022

3.5.1.2 Recabar los datos de cada habitante de su vivienda, con nombre, tipo de sangre, número de teléfono celular, de oficina o escuela, así como la marca, color y número de placa de su vehículo. En el caso de menores de edad, los nombres y números de teléfono de sus amigos más cercanos de casa y escuela. Mantenga esta información en un lugar seguro y cerca de usted.

3.5.1.3 Vaciar periódicamente la memoria de su celular (mensajes, fotos, audios) para que en caso de robo o extravío no puedan usar esta información en tu contra.

3.5.1.4 No utilizar parentescos para identificar a sus familiares en la agenda de contactos de su celular, identifíquelos por su nombre, como a cualquier otro contacto.

3.5.1.5 No proporcionar tus datos o de sus conocidos a personas extrañas.

3.5.1.6 No exhibir datos personales en perfiles abiertos de redes sociales y evita al máximo ingresar sus datos personales en computadoras de uso compartido.

3.5.1.7 Al hacer pagos o transferencias bancarias por internet, verificar el sitio en que se hará. Buscar un icono de candado en las esquinas inferiores.

3.5.1.8 Prevéngase, ya que han sido detectadas bandas delictivas dedicadas a la extorsión telefónica, operando en grupos que obtienen los datos de sus víctimas a través de:

3.5.1.8.1 Directorios telefónicos públicos y especializados.

3.5.1.8.2 Falsas encuestas telefónicas y callejeras a estudiantes, amas de casa y ancianos.

3.5.1.8.3 Tarjetas de presentación obtenidas en ferias y exposiciones.

3.5.1.8.4 Robo de recibos telefónicos y otros estados de cuenta.

3.5.1.8.5 Solicitud de informes directamente en las sucursales.

3.5.1.8.6 Llenado de falsas solicitudes de crédito o invitación a rifas de viajes.

3.5.1.8.7 Promociones a jóvenes para recibir discos compactos, videos, etc.

3.5.1.8.8 Vigilancia en casetas telefónicas. Haciendo fila atrás de la persona que está usando el teléfono, escuchan su conversación y obtienen el nombre de la persona y determinan si la llamada está siendo efectuada a un familiar.

3.5.1.8.9 Uso del internet para obtener información, como de algún blog, cuentas de Twitter, Facebook, WhatsApp, o de alguna otra página donde hayan ingresado sus datos personales.

3.5.2 Durante.

3.5.2.1 Si acude a la sucursal un usuario que va a realizar una operación relacionada con el delito de extorsión, trate de tranquilizarlo y sugiérale que se comunique con su

REVISADO - 9 DIC. 2022

familiar para asegurarse de que todo esté en orden y evitar así el pago solicitado. Además, se le debe recomendar que acuda inmediatamente a denunciar los hechos ante las autoridades judiciales correspondientes, por presumirse que pueden ser constitutivos de delitos perpetrados con recursos de procedencia ilícita. Para el caso que el usuario haya realizado la operación, deberá informar inmediatamente lo sucedido al Oficial de Cumplimiento de Telecomunicaciones de México y a la Dirección de la Red de Sucursales, mediante correo electrónico.

3.5.2.2 Al recibir una llamada de extorsión se debe inmediatamente colgar el teléfono.

3.5.2.3 Si recibe una nueva llamada amenazante, responde que es número equivocado y cuelga.

3.5.2.4 Si le envían un correo con amenazas o intento de extorsión, bloquee la cuenta de quién se lo envía e infórmelo vía correo electrónico a la Gerencia Regional y/o Estatal y a la Dirección de la Unidad Estratégica de Inteligencia, así como a la Dirección de la Red de Sucursales.

3.5.2.5 Por ningún motivo proporcione datos personales o información del manejo de la sucursal que no sea necesaria a la persona que está del otro lado de la línea.

3.5.2.6 No intente negociar.

3.5.2.7 No se alarme, trate de permanecer tranquilo, ya que esto altera los sentidos y no deja pensar con claridad, además que mostrar miedo puede ser la mayor arma de los delincuentes en su contra.

3.4.3 Después.

3.5.3.1 Deberá dar aviso inmediatamente a la autoridad correspondiente en su estado y/o municipio, a fin de que se lleve a cabo la intervención policial y se logre ubicar a las personas. Posteriormente deberá interponer la denuncia ante el ministerio público federal y de aviso mediante correo electrónico a la Gerencia Regional y/o Estatal y a la Dirección de la Unidad Estratégica de Inteligencia, en un máximo de una hora.

3.5.3.2 Si en la sucursal se cuenta con identificador de llamadas, anote el número telefónico entrante, el sexo de la persona que llama, su acento, su tipo de lenguaje y cualquier otro dato que te parezca importante.

3.5.3.3 Si recibe una nota extorsiva por escrito, evite que el documento pase por varias manos; maneje el documento prudentemente de forma tal que las huellas del autor, en caso de quedar impresas, no sean borradas. Entregue el documento a las autoridades para su análisis técnico.

3.5.3.4 Cuando el mensaje se recibe electrónicamente, se procede de igual manera que el punto anterior, pero confirmando por teléfono y no se elimina el mensaje original hasta que quien asuma la coordinación de la atención del evento, lo autorice. Esto busca facilitar las labores de investigación de las autoridades.

3.5.3.5 Siempre ante cualquier amenaza y versión que le manejen vía telefónica, verifique que su familia esté bien.

REVISADO - 9 DIC. 2022

3.5.3.6 No se desespere ni acuda a entregar dinero o realizar depósitos bancarios, ni mucho menos utilizar los recursos del Organismo para realizar pagos por extorsiones de cualquier tipo.

3.5.3.7 Platique en conjunto con el personal de la sucursal y con su familia sobre las precauciones a seguir.

3.6 EN CASO DE DETECTAR UN FALTANTE EN CAJA.

Con el propósito de mantener actualizado el registro de incidencia y daños económicos contra el Organismo, generados por las personas servidoras públicas a los cuales les son detectados faltantes en caja en las diversas sucursales que integra la red de sucursales, es necesario que los titulares de las Gerencias Regionales y/o Estatales, informen de manera inmediata sobre éstos casos detectados a los titulares de las Direcciones de la Unidad Estratégica de Inteligencia, de la Red de Sucursales, de Asuntos Jurídicos y del Órgano Interno de Control en TELECOMM, mediante un comunicado electrónico inicial, con los datos básicos de circunstancias de modo, tiempo y lugar con los que cuenten en ese momento; para después ser formalizado en un plazo no mayor a cinco días naturales después de la detección de la irregularidad, mediante un informe escrito y firmado por el titular de la Gerencia Regional y/o Estatal al que corresponda la sucursal afectada, que contenga los siguientes datos:

- Nombre y registro de la sucursal.
- Fecha de detección.
- Nombre completo del presunto responsable y su cargo.
- Monto exacto del faltante, así como si fue reintegrado, en caso afirmativo indicar la fecha, el monto y el folio del recibo oficial o el mecanismo de ingreso del numerario.
- Fecha de levantamiento del Acta Circunstanciada y de la instrumentación del Acta Administrativa.
- Breve descripción de los hechos (la forma en que fue detectado el faltante, el argumento del presunto responsable sobre éste, en caso de que el empleado no haya reintegrado el efectivo de inmediato, mencionar el motivo y si existe algún compromiso de pago, las medidas precautorias –por ejemplo, relevar al empleado de sus funciones y del manejo de numerario- que se tomaron respecto al empleado al que se le detectó la irregularidad, así como cualquier dato que considere importante informar).

Asimismo, con relación a probables conductas irregulares que incurran las personas servidoras públicas con motivo de las diferencias identificadas de recursos en caja, los titulares de las Gerencias Regionales y/o Estatales, deberán presentar la denuncia, en los caso que así proceda ante la autoridad correspondiente, así como al Órgano Interno de Control en TELECOMM, con los datos o indicios que permitan advertir la presunta responsabilidad administrativa por la comisión de Faltas Administrativas.

Posteriormente, conforme se generen las documentales, deberán remitir una copia vía correo electrónico, a fin de que se actualicen los datos de cada uno de los asuntos reportados, como son:

- En caso de existir el reintegro de la cantidad total o parcial del faltante detectado (señalando la fecha, el monto y el folio del recibo oficial o el mecanismo de ingreso del numerario).
- Contenido del dictamen emitido por áreas centrales (Gerencia de Relaciones Laborales o Dirección de Asuntos Jurídicos), indicando en su caso el tipo de sanción emitida: rescisión laboral (fecha) y/o suspensión en sueldo y funciones (por cuantos días y el periodo de cumplimiento), etc., en caso de no haber sido acreedor a una sanción, indicar el motivo del

REVISADO - 9 DIC. 2022

área que lo emita (ejemplo prescripción o documentación mal integrada, etc.); o el resultado de la conducta, como lo es la presentación de su renuncia por parte del propio empleado.

- En caso de presentar Denuncia de Hechos, señalar ante que autoridad, la fecha y el número de Carpeta de Investigación; en caso de que exista la decisión de no presentarla, indicar el motivo.
- Respecto a estos casos, deberán notificar cualquier dato relevante respecto a la situación jurídica de la persona servidora pública denunciada penalmente.

3.7 ACCIONES A EMPRENDER ANTE UNA AMENAZA DE BOMBA.

Las presentes políticas serán de aplicación a cuantos avisos de bomba se reciban en cada una de las sucursales del Organismo, con total independencia del medio a través del cual se tenga conocimiento de los mismos, sea verbalmente a través de teléfono, o por escrito, cualquiera que sea su soporte o formato.

3.7.1 Antes.

3.7.1.1 El personal que conteste teléfonos en las sucursales, deberá conocer el procedimiento para el tratamiento de una amenaza de bomba (incluido en el Programa Interno de Protección Civil de la Unidad Administrativa).

3.7.1.2 Aplicar el protocolo con información preestablecida que permita a quien conteste el teléfono, tratar de obtener la información que éste requiera para su análisis posterior.

3.7.1.3 El personal deberá conocer a detalle su área de trabajo para que en caso de que en forma súbita y sin conocimiento previo, detecte cualquier elemento que le sea ajeno a su ámbito y le resulte sospechoso, lo notifique de inmediato la persona a cargo de la sucursal o de brigada para la evaluación del caso.

3.7.1.4 En ningún caso deberá ser movido o tocado cualquier bulto, maleta, portafolio o elemento sospechoso por personal de la sucursal, debiendo avisar de inmediato al jefe de brigada de la Gerencia Regional y/o Estatal y esperar instrucciones.

3.7.2 Durante.

3.7.2.1 Si es escrita: Tratar de no manipular ni destruir la nota, anotar la hora y lugar en donde la encontró, su procedencia y características de la persona que la entregó, en caso de que disponga de esta información.

3.7.2.2 Si es por vía telefónica. Atienda cortésmente y sin nerviosismo, no interrumpir al interlocutor, tratar de hacer razonar a la persona que amenaza para que cambie de actitud, anotar la hora en que la recibe, mantenga el mayor tiempo posible la comunicación e intente realizar las siguientes preguntas (Ver modelo 2).

3.7.2.3 En caso de recibir una amenaza no se debe discutir con el agresor y tratar de obtener la mayor información posible.

3.7.2.4 Una vez que el agresor colgó, la persona que recibió la llamada telefónica deberá informar rápidamente a la persona a cargo de la sucursal o de brigada. La persona que recibió la llamada deberá abstenerse de divulgar la información recibida.

REVISADO - 9 DIC. 2022

3.7.2.5 La persona a cargo de la sucursal o de brigada, solicitará al personal que realice rápida y discretamente una revisión de su área de trabajo, tratando de identificar objetos o bultos sospechosos. La revisión deberá realizarse observando con detalle los plafones, macetones, parte baja de muebles, cestos de basura, etc.

3.7.2.6 Si se identifica algún objeto sospechoso, deberá alejarse al personal y al público usuario de la zona, evitando tocar o mover dicho objeto.

3.7.2.7 Deberá informar de inmediato el hallazgo a la Gerencia de Monitoreo y Video Vigilancia y atender las instrucciones que se le den.

3.7.2.8 Una vez que el personal de seguridad acuda a la sucursal, la persona a cargo de la sucursal o de brigada deberá informar los detalles de lo que ha ocurrido y acatar las instrucciones que le indiquen.

3.7.2.9 Si el personal de seguridad decide que es necesario evacuar la sucursal, deberá aplicar el procedimiento respectivo (incluido en el Programa Interno de Protección Civil de la Unidad Administrativa).

3.7.3 Después.

3.7.3.1 Una vez concluida la situación de emergencia y que el personal de seguridad proporcione la indicación de que se puede ingresar nuevamente a la sucursal la persona a cargo de la sucursal deberá realizar un informe y enviarlo a la Dirección de la Unidad Estratégica de Inteligencia en un plazo que no excederá de 48 horas.

3.7.3.2 En caso de que se determine el no reingreso a la sucursal, la persona a cargo de la sucursal o de brigada deberá pedir instrucciones específicas de situación futura a su Gerencia Regional y/o Estatal.

4. PROTOCOLO PARA REPORTAR UN ILÍCITO.

Los responsables de la sucursal o el personal que presenció un acto delictivo deberán adoptar las siguientes líneas para reportar los hechos:

4.1. Una vez concluido el hecho delictivo, la persona a cargo de la sucursal, deberá reportar los hechos a la autoridad de seguridad pública más cercana.

4.2. Después, dará aviso vía telefónica a la Gerencia Regional y/o Estatal, para que a su vez estos informen a la Dirección de la Unidad Estratégica de Inteligencia.

4.3. Una vez que la DUEI haya recibido el reporte, con objeto de recabar información, personal de su adscripción, contactará vía telefónica las veces que sea necesario.

4.4. Posteriormente, el mismo día de los hechos, la persona a cargo de la sucursal o el trabajador que haya presenciado el acto delictivo, deberá elaborar una narrativa a puño y letra, misma que entregará al Coordinador de Supervisión, una vez que se presente al levantamiento de las actas correspondientes.

REVISADO - 9 DIC. 2022

CAPÍTULO SEXTO

VI. ANÁLISIS Y GESTIÓN DE RIESGOS.

1. DEFINICIÓN.

El análisis del riesgo es una herramienta de gestión cuyos patrones para medir están determinados por lo que se estima aceptable con respecto a las pérdidas incurridas. Para proceder de forma lógica y realizar un análisis de riesgo, es necesario llevar a cabo de antemano algunas tareas básicas:

a) Identificar los bienes que necesitan protección (dinero contenido en ventanillas, caja fuerte, cofre de seguridad, equipo informático, etc.).
b) Identificar los tipos de riesgos que pueden afectar los bienes involucrados (robo por intrusión, asalto dentro de la sucursal, asalto durante programas sociales, daño a las instalaciones, etc.).
c) Calcular la probabilidad de incidencia del riesgo.
d) Determinar el impacto o el efecto si ocurriera una pérdida determinada (física, de instalaciones o personal, monetaria).

2. OBJETIVO.

Evaluar el nivel de riesgo de las sucursales por parte de la Dirección de la Unidad Estratégica de Inteligencia, a fin de proponer la conveniencia de adaptar sistemas de disuasión, o en su defecto, proponer la reubicación o cierre definitivo de sucursal, tomando como base las estadísticas de ilícitos registrados en cada entidad.

3. BENEFICIOS DE UN ANÁLISIS DE RIESGOS

a) El análisis mostrará el nivel actual de seguridad de cada sucursal.
b) Destacará aquellas áreas o zonas donde se necesita más seguridad.
c) Ayudará a reunir algunos de los hechos necesarios para desarrollar y justificar contramedidas preventivas rentables.
d) Servirá para incrementar la necesidad de seguridad a través de valorar los puntos fuertes y débiles en su infraestructura.

4. PROCEDIMIENTO PARA DETERMINAR EL PORCENTAJE DE SINIESTRALIDAD.

4.1. Porcentaje de siniestralidad en sucursales a nivel nacional.

$$\%\ \text{índice de robos} = \frac{\text{(Número total de robos/asaltos en sucursales a nivel nacional X 100)}}{\text{Número total Robo/asalto de bienes o dinero a nivel nacional (Dato de INEGI)}}$$

4.2. Porcentaje de siniestralidad por Estado.

$$\%\ \text{índice de robos} = \frac{\text{(Número total de robos/asaltos en sucursales por estado X 100)}}{\text{Número total de robos/asaltos a nivel nacional en la red de sucursales}}$$

REVISADO - 9 DIC. 2022

5. ESTUDIO DE SEGURIDAD.

Para estar en capacidad de responder a cualquier riesgo presente o potencial en las sucursales, éstos deben ser previamente identificados. Una medida que la Dirección de la Unidad Estratégica de Inteligencia adoptará para lograr esta tarea, es la realización de estudios de seguridad. Estos servirán para realizar una evaluación en sitio, para determinar el estado actual de seguridad, identificar vulnerabilidades, determinar la necesidad de protección y hacer recomendaciones para mejorar la seguridad de conjunto.

Para realizar estos estudios las Gerencias Regionales y/o Estatales deberán prever lo siguiente:

5.1 Solo el personal designado por el titular de la Dirección de la Unidad Estratégica de Inteligencia podrá realizar los estudios de seguridad con el objetivo de analizar la situación que prevalece en las sucursales.

5.2 Durante el desarrollo de los estudios, el personal designado tendrá la facultad de visitar las instalaciones de las sucursales, analizar la infraestructura y entrevistar al personal.

5.3 Al término del estudio, se presentará al titular de la Dirección de la Unidad Estratégica de Inteligencia la evaluación de las medidas de protección discutidas en los hallazgos encontrados, la identificación de vulnerabilidades específicas (en orden de importancia) y el grado de seguridad que requiere.

5.4 Por último se emitirán a las Gerencias Regionales y/o Estatales, recomendaciones específicas para la utilización adecuada de los equipos, controles administrativos, implementación de medidas de protección, reforzamiento de las medidas de seguridad ya existentes, etc. Dependiendo del objetivo específico del estudio y de las condiciones en que se encuentren los inmuebles.

5.5 Serán las Gerencias Regionales y/o Estatales, las encargadas de implementar las recomendaciones que emita el titular de la Dirección de la Unidad Estratégica de Inteligencia e informar con evidencia documental las acciones emprendidas cuyo cumplimiento deberá ser supervisado por la Dirección de la Red de Sucursales.

6. GESTIÓN DEL RIESGO DEFINIDO.

Es muy importante que después de haber identificado, analizado y evaluado los riesgos existentes en cada sucursal, se seleccione un tratamiento para reducir pérdidas potenciales.

El análisis debe contar dónde, cuándo y cómo es probable que el riesgo se materialice. Debe también decir la extensión del daño.

6.1. El riesgo puede evitarse, eliminarse o reducirse a unas proporciones manejables.

Se realizará mediante la implementación de procedimientos de seguridad de vidas, bienes materiales y equipos, que elimine o reduzca el problema.

6.2. El riesgo puede asumirse o retenerse.

Al asumir el riesgo, las Gerencias Regionales y/o Estatales se obligan a la pérdida en que se incurra. Si la pérdida potencial se encuentra entre los límites que se espera y por otra parte esta es aceptable, el riesgo puede reconocerse por lo que es y dejarlo así. No se hace ningún

REVISADO - 9 DIC. 2022

esfuerzo para controlar, eliminar o minimizar el riesgo. Ninguna acción se toma para corregir la situación.

6.3 El riesgo puede transferirse a un tercero.

Cuando se transfiere un riesgo, el gestor del riesgo, se debe esforzar por obtener un programa de seguros disponible. Esta tarea incluye, entre otras cosas, determinar las mejores primas y más deducibles disponibles.

REVISADO - 9 DIC. 2022

CAPÍTULO SÉPTIMO

VII. PROHIBICIONES Y SUPERVISIÓN.

Serán las personas titulares de las Gerencias Regionales y/o Estatales quienes, en coordinación con la Dirección de la Unidad Estratégica de Inteligencia, se encarguen de supervisar la debida aplicación de este tema.

1. PROHIBICIONES.

1.1. DEFINICIÓN.

Las distintas operaciones que se realizan dentro de una sucursal requieren de la confidencialidad y discreción propias del tipo de transacciones ahí realizadas y que generalmente están relacionadas con aspectos donde el dinero en efectivo es el producto que se intercambia. Por ello resulta fundamental el que, el público usuario pueda realizar sus operaciones dentro de un entorno de seguridad, que le ofrezca la tranquilidad de realizar éstas en forma privada y que de ninguna forma pueda comunicarse el motivo y/o monto de la operación a terceras personas, dentro o fuera de la sucursal.

1.2. PROHIBICIONES.

1.2.1 Para efectos de apoyar lo anterior, está prohibido para el personal de la sucursal y público usuario, el uso de teléfonos celulares y/o cualquier otro tipo de comunicación móvil dentro de las instalaciones de la misma, para lo cual se llevarán a cabo las siguientes acciones:

- Indicar claramente dicha prohibición de uso, mediante la colocación de señalizaciones disuasivas, tanto en la puerta principal de ingreso como en la zona de ambulatorio.
- Esta prohibición será extensiva al personal y prestadores de servicios externos, excepto cuando por razones de su actividad, deban utilizar estos medios de comunicación (seguridad y mantenimiento).
- La persona a cargo de la sucursal deberá informar a las personas que hagan uso de sus teléfonos celulares dentro del inmueble, la prohibición establecida y su finalidad de brindar seguridad en beneficio de todos.
- Si cuenta con facilidades de comunicación hacia el exterior y si la persona que requiere comunicarse es un usuario reconocido, se le podrá ofrecer este apoyo para que se dé cumplimiento a la prohibición sin afectar las relaciones con estos.

1.2.2 Personas ajenas que permanezcan demasiado tiempo en la sucursal, sin realizar ninguna transacción, ni pedir un servicio a los operadores y operadoras de la misma.

- Se deberá invitar a los usuarios que se encuentren al interior de la sucursal sin realizar algún tipo de transacción de forma sutil y atenta, que no puede permanecer por cuestiones de seguridad al interior de la sucursal.
- Se debe mantener una vigilancia visual sobre personas que permanezcan mucho tiempo en la sucursal y más si muestran nerviosismo, irritabilidad o realizan constantes movimientos (sentarse, pararse, caminar, volver a sentarse, etc.)
- Se extremará la vigilancia visual sobre esas personas, sobre todo si realizan movimientos de las manos hacia la cintura, esto podría ser indicio de que tienen alguna arma y está por sacarla.

REVISADO - 9 DIC. 2022

- Cuando personas extrañas permanezcan más de 15 minutos sin realizar ningún trámite, deberán dar aviso a la seguridad con que se cuenta o bien informar a las autoridades federales, estatales o municipales que se encuentren lo más cerca de la sucursal.

1.2.3 No se deberá permitir el acceso a las sucursales en ninguna de sus áreas, a vendedores ambulantes o de cualquier persona ajena a la misma.

- Bajo ninguna circunstancia se permitirá el acceso al interior de la sucursal de vendedores ambulantes o persona desconocida, ya que estos pueden ser cómplices de asaltantes, o hampones que puedan poner en peligro la integridad física de los trabajadores y de los usuarios y en riesgo los recursos económicos que maneje dicha sucursal.

1.2.4 Está prohibida la permanencia de familiares en la sucursal en horas de labores.

- Evitar la permanencia de familiares, especialmente menores de edad en el interior de la sucursal, lo cual tiene por objeto evitar poner en peligro en un momento determinado a esas personas en caso de asalto, o bien que puedan ser tomados como rehenes y así obligar a la persona a cargo de la sucursal a entregar los recursos monetarios en existencia.

1.2.5 Evitar llevar aparatos u objetos ajenos a la sucursal como:

- Televisiones, audífonos, radios, cafeteras, estufas, parrillas, encender velas o veladoras y cualquier equipo u objeto ajeno a los enceres que han sido proporcionados como instrumentos de trabajo por TELECOMM, esto, con la finalidad de evitar que se distraigan de las funciones que realizan y se pierda la atención al público, así como prevenir o minimizar el riesgo de incendio.

1.2.6 No cambiar dinero por denominaciones de menor o mayor valor.

- El personal de las sucursales tienen estrictamente prohibido realizar cambio de dinero por denominaciones de menor o mayor valor a cualquier persona que solicite este tipo de operaciones. Esto evitará sacar dinero de forma innecesaria y que el personal caiga en distracciones.

1.2.7 Evitar portar objetos o artículos ostentosos o de valor.

- Se recomienda al personal, evitar portar joyas ostentosas, relojes, bolsos, artículos llamativos como reproductores de música, celulares y demás, que estén fácilmente visibles al público y que puedan motivar la actuación de los delincuentes y propicien la exposición al riesgo.

1.2.8 No difundir información confidencial sobre la operación de las sucursales.

- El personal de las sucursales deberán evitar en todo momento la fuga de información sobre los procedimientos de operación, modalidades de transferencia de dinero, números de cuenta, claves de operadores, horarios de recolección y entrega de valores y sumas que se manejan en cada una de ellas.

1.2.9 No dejar dinero a la vista del público usuario.

REVISADO - 9 DIC. 2022

- Los empleados de ventanilla evitarán dejar a la vista del público usuario dinero que llame la atención, con el objeto de evitar posibles asaltos.
- Los empleados de ventanilla y/o la persona a cargo de la sucursal bajo ninguna circunstancia realizarán el conteo de efectivo en el área de ventanilla y frente a los usuarios.

1.2.10 Área interna de la sucursal.

- Durante la operación de la sucursal y hasta su cierre, está estrictamente prohibido abrir la puerta que da acceso del ambulatorio hacía el área interna de la sucursal.

- La persona a cargo de la sucursal es el único facultado para abrir esta puerta, siempre que sea plenamente justificado (casos de emergencia), o por alguna actividad propia de sus funciones.

2. SUPERVISIÓN.

2.1. POLÍTICAS.

2.1.1 Con la finalidad de preservar la seguridad y protección de sucursales, resulta indispensable el establecimiento de mecanismos y procesos que permitan prevenir y disuadir actos delictivos, en virtud del incremento y aparición de nuevos modos de operación de delincuencia cometidos en perjuicio del público usuario y de las Instituciones, así como del personal y patrimonio de las mismas.

2.1.2 En consecuencia, la Dirección de la Unidad Estratégica de Inteligencia deberá coordinarse con las Gerencias Regionales y/o Estatales, a fin de que las sucursales cumplan con los procedimientos y medidas básicas de seguridad, así como con las características, y especificaciones sobre materiales, dimensiones y calidad de aquellos recursos con que deben contener las instalaciones.

2.1.3 Para tales efectos, es necesario que los funcionarios y empleados de la Institución, conozcan y lleven a cabo una debida observancia de los procesos de operación de la seguridad y protección de la sucursal.

2.1.4 Por su parte, el administrador o gerente designado para vigilar el cumplimiento de las normas sobre seguridad y protección, será el responsable de asegurar la correcta aplicación de estas por parte del personal que ahí labora.

2.2 FACULTADES DE SUPERVISIÓN DE LA DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA.

La Dirección de la Unidad Estratégica de Inteligencia llevará a cabo visitas de inspección y supervisión a las sucursales con el objeto de observar:

2.2.1 El debido cumplimiento de las Políticas en lo general, así como la implementación de las Medidas Básicas de Seguridad en lo particular.

2.2.2 La debida observancia e implementación en cada sucursal de los aspectos fundamentales para la seguridad de las mismas, establecidos en el presente documento.

REVISADO - 9 DIC. 2022

2.2.3 La conveniencia de prevenir prácticas tendientes a socavar la efectividad de las disposiciones contenidas en las políticas.

2.2.4 Con base en lo anterior, los titulares de las Gerencias Regionales y Estatales, supervisores, la persona a cargo de la sucursal y encargados de ventanilla deberán prestar todo el apoyo que el personal designado requiera, proporcionando los datos, informes y en general la documentación que los mismos estimen necesaria para el cumplimiento de su cometido, pudiendo tener acceso a sus Instalaciones.

2.2.5 En la documentación a que se refiere el numeral anterior, queda comprendida la información contenida en los sistemas automatizados de procesamiento y conservación de datos, así como cualesquiera otros procedimientos de tipo técnico, establecidos para ese objeto.

2.2.6 Es importante señalar que el personal designado por el titular de la Dirección de la Unidad Estratégica de Inteligencia llevará a cabo la práctica de las visitas, únicamente cuando éste presente al funcionario de mayor nivel de la sucursal, un oficio en el que se señale, entre otros aspectos, el carácter de las mismas, las disposiciones legales en que se fundan, así como el nombre de las personas que practicarán la visita. La práctica de la visita se iniciará aun cuando no esté presente el funcionario o persona a quien deba entregarse el oficio de notificación, caso en el que el supervisor hará la notificación al funcionario o empleado de mayor jerarquía que esté presente en la sucursal, o a aquél con el que pueda comunicarse de inmediato, identificándose debidamente y entregando el oficio a que se refiere el numeral anterior.

2.2.7 Como resultado de cada supervisión practicada, el personal designado por el titular de la Dirección de la Unidad Estratégica de Inteligencia elaborará un informe que hará del conocimiento del Gerente Regional y/o Estatal, supervisor o responsables de sucursal, remitiéndolo por oficio a la Dirección de la Red de Sucursales.

2.2.8 El personal designado por el titular de la Dirección de la Unidad Estratégica de Inteligencia podrá efectuar visitas de investigación que tengan como propósito aclarar una situación específica, a efecto de verificar el cumplimiento por parte de las Gerencias Regionales y/o Estatales, supervisores(as) y la persona a cargo de la sucursal, a las observaciones que haya formulado.

2.2.9 Para elaborar el informe de actividades, el personal designado por el titular de la Dirección de la Unidad Estratégica de Inteligencia tomará en consideración los siguientes aspectos:

a) El grado de incumplimiento de las medidas básicas de seguridad.
b) Las condiciones de las sucursales.
c) La reincidencia del área visitada.

REVISADO - 9 DIC. 2022

CAPÍTULO OCTAVO

VIII. CONDICIONES EXTERNAS DE LAS SUCURSALES EN MEDIDAS BÁSICAS DE SEGURIDAD.

Las Gerencias Regionales y/o Estatales apoyaran a la Dirección de la Unidad Estratégica de Inteligencia en la vigilancia y supervisión del tipo y nivel de riesgo a que están expuestas las sucursales, así como en la aplicación de medidas preventivas para brindar la seguridad necesaria, contando con la opinión de los(as) trabajadores(as) de estas.

1. ÁREAS CIRCUNDANTES.

1.1 DEFINICIÓN.

Se deberá entender por áreas circundantes a la sucursal, el entorno en el cual se encuentra ubicada, con el fin de definir el tipo y nivel de riesgos a los que está expuesta y para establecer las precauciones y/o medidas adicionales de seguridad que deben observarse durante las labores cotidianas, o ante una emergencia que amenace a las personas y bienes que se encuentren en el interior y/o su operación normal.

1.2 CONOCIMIENTO.

La persona a cargo de la sucursal deberá conocer el entorno de la vía pública y reportar al titular de la Gerencia Regional y/o Estatal, a la Dirección de la Red de Sucursales y a la Dirección de la Unidad Estratégica de Inteligencia, las condiciones de riesgo que pudieran afectar a los empleados y al público usuario, tales como puestos ambulantes, vehículos abandonados, indigentes y personas en actitud sospechosa, entre otros.

2. PUESTOS AMBULANTES, FIJOS O SEMIFIJOS.

2.1 La persona a cargo de la sucursal deberá reportar a la Dirección de la Unidad Estratégica de Inteligencia, el establecimiento de puestos fijos o semifijos, vendedores ambulantes o tianguis, ubicados frente a ella, y si considera que son un riesgo para la seguridad, tomará acciones a fin de que su presencia sea reportada a las autoridades administrativas correspondientes y se sugiera su reubicación en puntos que no representen un riesgo.

2.2 Cuando la instalación de puestos ambulantes se esté generando como un acto nuevo de las personas dedicadas a estas actividades, se dará aviso de inmediato a la Dirección de la Unidad Estratégica de Inteligencia, a efecto de que se giren las instrucciones adecuadas y/o se inicien gestiones oportunas ante las autoridades competentes para evitar el asentamiento de los puestos.

En ambos casos la persona a cargo de la sucursal conservará la comprobación documental de las acciones realizadas ante las autoridades correspondientes.

3. ESTACIONAMIENTO DE VEHÍCULOS.

El estacionamiento de vehículos en el frente de la sucursal deberá ser considerado como un factor de riesgo para su seguridad, motivo por el cual se procurará obtener de las autoridades de seguridad pública o de tránsito y vialidad, la prohibición de estacionarse en esta zona o bien su autorización para que sea señalizada como área exclusiva para maniobras de los vehículos de las empresas transportadoras de valores.

REVISADO - 9 DIC. 2022

3.1 SUPERVISIÓN DE LAS PERSONAS RESPONSABLES DE SUCURSALES.

Considerando que las funciones básicas de las personas responsables de sucursales están orientadas a la atención de los clientes y del público usuario, los funcionarios y las funcionarias que atiendan estos puestos procurarán ubicarse estratégicamente en la misma para poder supervisar adecuadamente el funcionamiento, debiendo ubicarse de acuerdo con los siguientes criterios:

3.1.1 Que su ubicación les permita mantener una visibilidad suficiente sobre la zona de influencia a fin de detectar cualquier alteración a las actividades normales.

3.1.2 Que sus sitios de trabajo se ubiquen al alcance del público usuario, pero en puntos que eviten que su seguridad personal sea vulnerada con relativa facilidad.

3.1.3 Que su ubicación esté a la vista del resto del personal, con el propósito de que se perciba cualquier acto contra sus personas.

3.1.4 Supervisión de las personas responsables de sucursales.

REVISADO - 9 DIC. 2022

IX. ANEXOS.

REVISADO - 9 DIC. 2022

GLOSARIO DE TÉRMINOS

CONCEPTO	DESCRIPCIÓN
ACCESO DIGITAL	Teclado electrónico para registrar, identificar y permitir un acceso mediante la aplicación de una clave personalizada. Se coloca normalmente para el control de acceso a las áreas restringidas.
ACTA ADMINISTRATIVA	Documento de control interno en las empresas que se elabora con la finalidad de señalar, dejar evidencia y/o sancionar hechos en los que el trabajador ha incurrido y que van en contra de la regulación normativa de la empresa como puede ser: la Ley Federal del trabajo, contrato colectivo o individual de trabajo, reglamento interno de trabajo o código de conducta establecidos.
ACTA CIRCUNSTANCIADA	Es el documento que se utiliza para asentar determinados hechos, con la finalidad de que quede constancia de estos para los efectos legales a que haya lugar y la firma de conocimiento de los involucrados en los hechos y al menos dos testigos de asistencia.
ALERTA	Situación de vigilancia o atención.
AMAGO	Es el aviso por parte del personal de la sucursal donde ingresa un código de emergencia para alertar al Centro Nacional de Monitoreo respecto a la existencia de un riesgo.
AMBULATORIO	Instalación semifija de dimensiones pequeñas que consta de al menos una sola ventanilla, mediante la cual se prestan la atención y servicios al público usuario.
AMENAZA	Circunstancia adversa que ofrece la voluntad manifiesta de causar daño o perjuicio a la operación, a instalaciones, personas y bienes del organismo.
ANTIVIRUS	Utilidad que examina el disco duro en busca de virus y elimina cualquiera que encuentre.
APLICACIÓN	Cada uno de los programas informáticos desarrollados para satisfacer una necesidad específica, que una vez ejecutados permiten trabajar con la computadora.
ASALTO	Es el apoderamiento de un bien ajeno, empleando la agresión y violencia física mediante el uso de armas de fuego o de cualquier otro objeto, para amedrentar o dañar la integridad física de quien posee o dispone del objeto.
AUDITAR	Examinar la contabilidad y los procedimientos de una entidad

REVISADO - 9 DIC. 2022

CONCEPTO	DESCRIPCIÓN
AUTO ROBO	Conducta ilícita perpetrada por el propio personal de la sucursal, aprovechando dolosamente el acceso a los recursos que le han sido encomendados para la operación Bancaria.
BOTÓN DE LIBERACIÓN	Dispositivo eléctrico para liberar la apertura de una puerta. Esta opción sólo funciona desde el interior de las zonas protegidas.
BOLEADO	Término que se utiliza para darle el acabado en las orillas y esquinas de un cristal para evitar que provoque lesiones a las personas.
CAJA FUERTE	Mueble cúbico de alta resistencia física, generalmente de acero de gran espesor, en cuyo interior se resguarda dinero en efectivo y valores. Cuentan con una puerta cuya chapa es de combinación.
CENTRAL DE MONITOREO	Instalación remota a la cual confluyen todas las señales de monitoreo y alarma que se generan en todas y cada una de las sucursales de la Institución.
CLAVE DE ACCESO	Combinación de letras, números y signos que debe teclearse para obtener acceso a un programa o partes de un programa determinado, una terminal o una computadora, un punto en la red, etc.
COFRE DE SEGURIDAD	Mueble cúbico de alta resistencia física, generalmente de acero de gran espesor, que cuenta con una puerta cuya chapa es de combinación, además de tener un dispositivo donde los servidores públicos de TELECOMM solo pueden ingresar dinero y el personal de la ETV, es quien cuenta con la combinación para retirarlo. Los cofres son propiedad de la referida ETV y cuentan con un seguro en caso de pérdidas.
CONDUCTA ILÍCITA	Comportamiento ilegal de una persona que afecta el patrimonio de las instituciones de crédito, al público usuario y/o al personal desde un punto de vista tanto físico como moral.
DESENCRIPTAR	Descifrado de un texto codificado mediante un algoritmo y protegido con una clave.
DISCO DURO	También conocido como unidad de almacenamiento. Elemento de reducidas dimensiones y muy manejable que se utiliza como dispositivo de almacenamiento de datos. Los discos o USB se introducen en un dispositivo para su lectura y grabación mediante el uso de una o varias cabezas lectoras-grabadoras magnéticas.
DISUADIR	Crear en el agresor un sentimiento de impotencia ante un sistema de seguridad.

CONCEPTO	DESCRIPCIÓN
EFECTIVO	Dinero ya sea en billetes o monedas, de curso legal, nacionales o extranjeras para realizar transacciones comerciales.
ENCRIPTACIÓN	Datos ocultos mediante una clave que permite la protección de información al aplicarles algoritmos matemáticos.
ENCRISTALAR VENTANILLAS DE OPERACIÓN	Dispositivo de seguridad colocado a manera de barrera en el mostrador de atención al público usuario mediante la colocación de un vidrio que impide el acceso a la zona restringida de servicios.
ENCUBRIMIENTO	Conducta delictiva consistente en participar en un delito con posterioridad a su ejecución o los que se sabe se están cometiendo, evitando el descubrimiento de sus autores o auxiliándolos para obtener los beneficios de su acción.
EQUIPO DE RADIOCOMUNICACIÓN	Son equipos que se utilizan para comunicarse a través del espacio por medio de ondas electromagnéticas.
ESTACIÓN	Conjunto de instalaciones que incluyen una mesa de trabajo, una terminal de computadora, los periféricos necesarios y accesorios y que están destinados a los usuarios de un sistema.
ETV	Empresa Trasladadora de Valores.
EXTORSIÓN	Presión que se ejerce sobre alguien mediante amenazas para obligarlo a actuar de determinada manera y obtener así dinero u otro beneficio.
FIRMWARE	El firmware o soporte lógico inalterable es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Está fuertemente integrado con la electrónica del dispositivo, es el software que tiene directa interacción con el hardware, siendo así el encargado de controlarlo para ejecutar correctamente las instrucciones externas.
FRAUDE	Engaño económico que se comete en perjuicio contra una persona u organización con el objeto de conseguir ilícitamente un beneficio.
GESTIÓN DE RIESGO	Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen la identificación, el análisis y la evaluación de riesgo.
GRABADOR DE VIDEO	Controlador de imágenes con la propiedad de presentarlas a través de un monitor en forma secuenciada.
GRABADOR DIGITAL	Dispositivo que toma las imágenes de video analógico generado por las cámaras del sistema de videovigilancia, las digitaliza y almacena en un medio magnético u óptico, como un archivo electrónico.
HARDWARE	Todos los equipos y periféricos que conforman el sistema de cómputo.

REVISADO - 9 DIC. 2022

CONCEPTO	DESCRIPCIÓN
HERMETISMO	Es la propiedad de aquello que resulta hermético: cerrado, inviolable, clausurado.
HURTO	Tomar, apoderarse o retener sin violencia bienes ajenos contra la voluntad de su dueño.
INFORMACIÓN NO AUTOMATIZADA	Toda aquella información impresa, visual o audible que no reside en un sistema informático.
INTIMIDACIÓN	El servidor público que, por sí, o por tercera persona, utilizando violencia física o moral, inhibe o intimide a cualquier persona para evitar que esta o un tercero denuncie, formule querella o aporte información relativa a la presunta comisión de una conducta sancionada por la legislación penal o por la Ley Federal de Responsabilidades de los Servidores Públicos.
INTRUSIÓN	Término que se aplica al robo de un lugar cerrado.
ILÍCITO	Conducta contraria a las leyes y/o a los ordenamientos administrativos del Organismo.
LINEAMIENTO	Son leyes, estatutos, reglamentos, planes, programas, proyectos, convenios, acuerdos y manuales.
LUZ ESTROBOSCÓPICA	Es una fuente luminosa que emite una serie de destellos muy breves en rápida sucesión y se usa para producir exposiciones múltiples de las fases de un movimiento. Su objetivo es disuadir a los intrusos e indicar a la policía donde se está cometiendo una infracción.
MECANISMOS DE RETARDO	Dispositivos físicos y electrónicos que tienen la función de abrir una puerta de seguridad en accesos, bóvedas o cajas fuertes, con un retardo previamente programado.
MEDIDAS DE SEGURIDAD	Son aquellas que eliminan o disminuyen el riesgo, minimizando la probabilidad de ocurrencia de un acto delictivo en contra del personal, usuarios y patrimonio del Organismo.
MEDIO AUTOMATIZADO	Elemento o dispositivo mecánico y/o electrónico por medio del cual se realiza una actividad de manera programada y repetitiva.
MEDIO MAGNÉTICO	Elemento físico con propiedades magnéticas que permite la grabación y reproducción de datos.
MÍSTICA DE SERVICIO	Es amor al trabajo, amor a la empresa, amor a los superiores, amor a los compañeros, amor a los dirigidos, amor a cada una de las cosas que conforman el medio ambiente que nos proporciona el vivir cada día con plenitud.

REVISADO - 9 DIC. 2022

CONCEPTO	DESCRIPCIÓN
MONITOR	Receptor de señal del sistema de videovigilancia.
MONITOREO	Visualización de cámaras vía web.
MODIFO	Movimiento Diario de Fondos. Es un sistema contable en el cual se registran los movimientos diarios de fondos de las sucursales de Telecomunicaciones de México, siendo responsabilidad de las personas a cargo de las sucursales la veracidad de la información de sus cierres que registren.
OSTENTOSO	Llamativo por su apariencia lujosa o aparatosa.
PROCEDIMIENTO	Conjunto de actividades para llevar a cabo una actividad o un proceso.
PROCESO	Secuencia de tareas de tareas que se llevan a cabo una detrás de la otra.
PROTOCOLO	Secuencia detallada de un proceso de actuación científica, técnica, médica, etc.
OFICIAL DE CUMPLIMIENTO	Funcionario que ocupa un cargo dentro de las tres jerarquías inmediatas inferiores a la del director general del transmisor de dinero del que se trate y será el enlace con la CNBV Y El COCOCO del transmisor de dinero y desempeñara las funciones a las que se refiere las diversas fracciones del numeral 36 de la DCG.
PAGADOR HABILITADO	Es el empleado designado para llevar a cabo los pagos a los beneficiarios de los programas sociales
PANEL DE ALARMAS	Dispositivo electrónico que supervisa el estado de los sensores de alarma (detectores de humo, de aviso de asalto, de ruptura de cristal, de movimiento, de temperatura, de vibración o apertura de puertas) y en caso de tener un evento de emergencia (asalto, intrusión o incendio), se comunica a través de las líneas telefónicas o la red de datos, para informar a la Central de Alarmas el acontecimiento.
PASSWORDS	Clave de acceso a un sistema informático.
PELIGRO	Situación de riesgo potencial o presente de que suceda un hecho adverso contra personas o bienes.
PERNOCTAR	Permanencia del efectivo en un lugar determinado posterior al cierre de operaciones.
PRECAUCIÓN	Cuidado, reserva, cautela para evitar o prevenir daños o inconvenientes.

REVISADO - 9 DIC. 2022

CONCEPTO	DESCRIPCIÓN
PREVENCIÓN DE RIESGOS	Medidas que se toman de manera anticipada para evitar que suceda un riesgo, y si el riesgo se produce, los daños sean los mínimos posibles.
PRIVILEGIOS	Excepción especial o exclusiva que se concede a alguien para ingresar a los sistemas informáticos. Los privilegios se acotan y controlan a través de las facultades específicas que determine el administrador del sistema.
PRIVILEGIOS DE ACCESO	Permisos definidos para que un usuario explote información de un sistema una vez que éste ha cubierto los requisitos para esta condición.
PRODUCTO DE INTELIGENCIA	Son los documentos generados por los analistas, resultado de la recolección de información, a través de diversas fuentes y herramientas, con el propósito de aportar elementos para la toma de decisiones.
PÚBLICO USUARIO	Aquellas personas que contratan o utilizan los servicios prestados por TELECOMM.
PUERTA BLINDADA	Elemento metálico de alta resistencia física con mirilla o ventanilla de cristal blindado que controla e impide cualquier acceso violento hacia el interior de las zonas protegidas.
RED	Conjunto de equipos de cómputo interconectados entre sí que comparten diversos recursos informáticos.
RED DE TELECOMUNICACIONES	El medio de comunicación por el cual son transmitidas las imágenes desde un grabador digital hasta la Central de Alarmas Institucional, el cual puede ser: • Comercial. • Red telefónica. • Microondas. • Radiofrecuencia. • Red Celular.
RED DE SUCURSALES	Conjunto de sucursales de Telecomunicaciones de México permanentes o temporales en la República Mexicana.
RIESGO	Posibilidad de que se dé un suceso que puede provocar afectación, para vidas, bienes o la continuidad de las actividades.
ROBO	Es un delito contra el patrimonio, consistente en el apoderamiento de bienes ajenos, con intención de lucrarse, empleando para ello fuerza en las cosas o bien violencia o intimidación en la persona.
RONDÍN	Recorrido realizado para la vigilancia por los elementos de las corporaciones de seguridad pública.

REVISADO - 9 DIC. 2022

CONCEPTO	DESCRIPCIÓN
SEGURIDAD	Ausencia de riesgo. Protección de personas y bienes contra todo tipo de daños, pérdidas o perjuicios derivados de la exposición de riesgo, así como la combinación del personal, medios y procedimientos para prevenir, contrarrestar, demorar o controlar las contingencias originadas por el hombre.
SEGURIDAD ELECTRÓNICA	Conjunto de elementos técnicos destinados a advertir localmente y/o a distancia de cualquier incidencia que pueda representar un riesgo. En las sucursales contempla la cámara de videovigilancia o el panel de alarma.
SEGURIDAD FÍSICA	Conjunto de elementos materiales que sirven de soporte a los sistemas electrónicos de seguridad y que obstaculizan una acción delictiva o el desarrollo de un siniestro.
SEGURIDAD LÓGICA	Aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo se permite acceder a ellos a las personas autorizadas para hacerlo.
SEGURIDAD Y PROTECCIÓN	El conjunto de medios humanos e instalaciones dirigidos a la prevención de riesgos, protección de bienes y personas y minimización de los daños.
SENSOR	Dispositivos electrónicos y/o mecánicos que detectan un cambio de condición en forma automática o manual y generan una señal de alarma al Centro Nacional de Monitoreo.
SEÑAL DE ALARMA	Mensaje local y remoto, luminoso, acústico o silencioso que avisa de la producción de un incidente o siniestro o de la posibilidad de que éste ocurra.
SEÑALIZACIÓN DISUASIVA	Mensajes que se colocan en sitios estratégicos de una sucursal, los cuales advierten sobre una condición de seguridad y protección.
SERVIDOR	Dispositivo de un sistema que resuelve las peticiones de otros elementos del sistema, denominados clientes.
SERVIDOR DE ACCESO A INTERNET	Equipo de cómputo que administra el sistema informático que controla el acceso de usuarios a la información, tanto de alarmas como de imágenes.
SERVIDOR DE BASE DE DATOS	Equipo de cómputo que recibe, almacena y administra los archivos de imágenes enviadas al Centro Nacional de Monitoreo.
SIGITEL	Sistema de Giros Telegráficos

REVISADO - 9 DIC. 2022

CONCEPTO	DESCRIPCIÓN
SINIESTRALIDAD	Indicador que representa la proporción de incidentes de una entidad, alcaldía o municipio respecto del total de sucursales existentes en la misma.
SINIESTRO	Avería, destrucción fortuita o pérdida importante que sufre el Organismo, en particular sus sucursales, el público usuario, los empleados de aquéllas o su patrimonio, por actos del hombre o hechos de la naturaleza que vulneren el buen funcionamiento de las medidas de seguridad.
SISTEMA DE DISUACIÓN	Conjunto de medidas de seguridad para eliminar o disminuir la ocurrencia de un evento delictivo.
SISTEMA LOCAL DE ALARMAS	Instalación local a la cual confluyen todas las señales de monitoreo y alarma que se generan en las sucursales y que se retransmiten al Centro Nacional de Monitoreo.
SISTEMAS DE MONITOREO Y ALARMA	Conjunto de elementos físicos y electrónicos que permiten probar periódicamente la condición de un sensor y que genera un aviso cuando las condiciones identificadas salen de los parámetros de control previamente definidos. Los sistemas consideran los controles locales y remotos, instalándose los primeros en las sucursales que tienen integradas las claves de apertura o cierre de estas; los segundos están colocados en centrales propias o de terceros y tienen como función recibir las señales que se generan y activar los mecanismos de respuesta.
SITUACIÓN CRÍTICA	Momento de riesgo que se encuentra en un nivel de peligro y fuera de control, el patrimonio del Organismo, el público usuario y/o el personal de la sucursal.
SOCAVAR	Debilitar algo o a alguien, especialmente en el aspecto moral.
SOFTWARE	Término genérico que designa al conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible operar la computadora.
SUCURSAL	Sucursales de Telecomunicaciones de México destinadas a la atención del público usuario, en donde se efectúan operaciones y se prestan servicios Telegráficos y bancarios con manejo de efectivo o
SUPERVISOR	Personal encargado de llevar a cabo las supervisiones en la red de sucursales.
TABLA DE ACCESO Y FACULTADES	Documento de control que define los privilegios de acceso y explotación de la información por parte de los usuarios de un sistema.

REVISADO - 9 DIC. 2022

CONCEPTO	DESCRIPCIÓN
TENTATIVA	Cuando, con el objetivo de cometer un delito, ha comenzado alguien su ejecución por medios apropiados, pero no se consuma por causas ajenas a su voluntad.
TITULAR	Es el administrador y responsable de cada sucursal
TRANSFER	Mecanismo blindado para la entrega y/o recepción de efectivo y valores. Este mecanismo no permite el contacto directo entre el personal de la sucursal y el personal de la compañía de traslado de valores.
UPS	Es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.
VALORES	Documentos, dinero, títulos, acciones u obligaciones que representan cierta suma de dinero y que generalmente son utilizados para realizar o amparar transacciones bancarias.
VEHÍCULO BLINDADO	Unidad de transporte de valores reforzada con placas metálicas de diferentes niveles de blindaje para la protección de sus contenidos y de la tripulación, operado por personal capacitado y armado.
VEHÍCULOS MOTRICES	Son los vehículos que tienen su potencia sobre el eje delantero.
VIGILANCIA REMOTA	Vigilancia visual que combina los beneficios analógicos de los tradicionales CCTV con las ventajas digitales de las redes de comunicación IP, permitiendo la supervisión local y/o remota de imágenes y audio, así como el tratamiento digital de las imágenes.
VIGILANTE	Persona que se mantiene en observación permanente para velar por algo.
VIRUS	Programa maligno que se instala o ejecuta en la computadora sin previo aviso y que puede corromper el resto de los programas, archivos de datos y el sistema operativo. Los virus se transmiten a través de disquetes, correo electrónico o Internet y se propagan pegando copias de sí mismo en otros programas compartidos en una red, es capaz de replicarse y paralizar muchas computadoras en poco tiempo.
ZONA DE RECUENTO	Área de acceso restringido que se utiliza para la recepción, recuento y entrega del efectivo que es concentrado o retirado de las sucursales.

REVISADO - 9 DIC. 2022

FORMATOS

REVISADO - 9 DIC. 2022

FORMATO DE MEDIDAS DE SEGURIDAD
TCM-9000-F09-22

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm

MEDIDAS DE SEGURIDAD EN SUCURSALES TELEGRÁFICAS					
DATOS GENERALES DE LA SUCURSAL				TRASLADO DE VALORES	
Nombre de sucursal:	Cuauhtémoc	Tipo de Sucursal:		Valores remesados por:	
Registro:	32035	Tipo de población:		Monto autorizado para el traslado por conducto personal:	
Estado:	Zacatecas	Dentro de un espacio público:		Cantidad de efectivo autorizada para mantener en ventanilla:	
Municipio:	Cuauhtémoc	Espacio designado:		Cantidad de efectivo autorizada para mantener en caja fuerte:	
Colonia/Localidad:	San Pedro Piedra Gorda	Tipo de inmueble:		Cantidad sugerida para incremento:	
Código postal:		Dirección (número exterior, número interior, código postal, y colonia):		Nivel de riesgo de la localidad:	
MOVIMIENTOS DE LA SUCURSAL					
¿Reapertura?		Fecha de reapertura:		Motivo de la reapertura:	
¿Reubicada?		Fecha de reubicación:		Motivo de la reubicación:	

TCM-9000-F09-22

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm

En caso de reapertura o reubicación, indique el nombre anterior de la sucursal:		En caso de reapertura o reubicación, indique el registro anterior de la sucursal:			

DATOS DEL PERSONAL ADSCRITO A LA SUCURSAL					
Número de personal adscrito a la sucursal:					
Nombre de los servidores públicos (Nombre(s) Apellidos)	Puesto que desempeña	Nombre de la plaza que ocupa	Nivel	Código de puesto	Fecha de ingreso al Organismo

TCM-9000-F09-22

REVISADO - 9 DIC. 2022

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm

GEOLOCALIZACIÓN Y DESCRIPCIÓN DEL ENTORNO	Coordenadas Latitud - Longitud:	

Insertar imagen del exterior de la sucursal	Insertar imagen de ventanillas	Insertar imagen del ambulatorio

Agregar

Insertar imagen del área de recuento	Insertar imagen de la o caja fuerte	Insertar captura de pantalla de la ubicación en Google Maps

Eliminar

TCM-9000-F09-22

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm

Colindancia:	
Frente a la sucursal	
Costado derecho	
Costado izquierdo	
Espaldas de la zucursal	

SEGURIDAD FÍSICA - Características del inmueble					
MATERIALES DE CONSTRUCCIÓN					
Material de construcción de los muros del inmueble:		Material de construcción del techo del inmueble:		Estacionamiento:	
Si tiene cortina metálica, indique su ubicación:		Material de la puerta del ambulatorio:		Piso:	
Número de puertas de acceso de la vía pública a la sucursal		Acometida eléctrica:		Baño:	
Total de puertas en la sucursal					

Descripción de la ubicación	Material de la puerta	Número de chpas de la puerta:	Material de la chapa 1:	Material de la chapa 2:	Material de la chapa 3:

TCM-9000-F09-22

REVISADO - 9 DIC. 2022

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm

CARACTERÍSTICAS DEL MOSTRADOR					
Material de construcción del mostrador:		Número de ventanillas de atención a usuarios:		Material de construcción de las ventanillas:	
La ventanilla cuenta con cajuela para documentos:		Espacio entre ventanilla y techo (Metros):		Observaciones y/o comentarios adicionales:	
CARACTERÍSTICAS DE LAS VENTANAS					
Número de ventanas exteriores en la sucursal:		¿Las ventanas internas tienen protección de varillas?:		Observaciones y/o comentarios adicionales:	
Número de ventanas internas en la sucursal:		¿Las ventanas externas tienen protección de varillas?:		Observaciones o comentarios adicionales:	
EQUIPO ELECTRÓNICO DE SEGURIDAD					
EQUIPO DE VIDEOVIGILANCIA					
Número de cámaras instaladas en la sucursal:	0				
Modelo / Marca	**Ubicación**	**Funciona correctamente**	**Tiene conexión con el Centro Nacional de Monitoreo:**	**Fecha de su última revisión**	**Observaciones**

TCM-9000-F09-22

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm

PANEL DE ALARMA					
Cuenta con panel de alarma:		Fecha de la última revisión:		Funciona correctamente:	
La alarma funciona correctamente:		Tiene botón de pánico:		Funcionan los magnetos de puertas y ventanas:	
Funcionan los sensores de movimiento:		Observaciones:			
RESGUARDO DE VALORES					
	SÍ/NO	**Ubicación**	**Descripción de la seguridad**		
Cofre de seguridad / Tómbola:					
Caja fuerte:					
Área de resguardo:					
RESGUARDO POLICIAL					
	SÍ/NO	**Empresa o corporación**	**Número de oficio de la Gestión**	**Número de oficio de respuesta de la**	**Frecuencia del resguardo policial**

TCM-9000-F09-22

REVISADO - 9 DIC. 2022

COMUNICACIONES Telecomm.

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

Vigilancia policial					
Convenio de seguridad con alguna autoridad local					

PROTECCIÓN CIVIL				
	SÍ/NO	Existencia	Localización	Necesidades
Extintores				
Equipamiento de identificación Protección Civil para el inmueble				
Señalización				
Botiquín de primeros auxilios				
UIPC (Unidad Interna de Protección Civil)				

TCM-9000-F09-22

FORMATO DE MEDIDAS DE SEGURIDAD
TCM-9000-F09-22

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm.

MEDIDAS DE SEGURIDAD EN SUCURSALES TELEGRÁFICAS					
DATOS GENERALES DE LA SUCURSAL				**TRASLADO DE VALORES**	
Nombre de sucursal:	1	Tipo de Sucursal:	7	Valores remesados por:	13
Registro:	2	Tipo de población:	8	Monto autorizado para el traslado por conducto personal:	14
Estado:	3	Dentro de un espacio público:	9	Cantidad de efectivo autorizada para mantener en ventanilla:	15
Municipio:	4	Espacio denegado:	10	Cantidad de efectivo autorizada para mantener en caja fuerte:	16
Colonia/Localidad:	5	Tipo de inmueble:	11	Cantidad sugerida para incremento:	17
Código postal:	6	Dirección (número exterior, número interior, código postal y colonia):	12	Nivel de riesgo de la localidad:	18
MOVIMIENTOS DE LA SUCURSAL					
¿Fue apertura?:	19	Fecha de reapertura:	20	Motivo de la reapertura:	21
¿Reubicada?	22	Fecha de reubicación:	23	Motivo de la reubicación:	24

TCM-9000-F09-22

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm.

En caso de reapertura o reubicación, indique el nombre anterior de la sucursal:	25	En caso de reapertura o reubicación, indique el registro anterior de la sucursal:	26		

DATOS DEL PERSONAL ADSCRITO A LA SUCURSAL					
Número de personal adscrito a la sucursal:	27				
Nombre de los servidores públicos (Nombre(s) Apellidos)	**Puesto que desempeña**	**Nombre de la plaza que ocupa**	**Nivel**	**Código de puesto**	**Fecha de ingreso al Organismo**
28	29	30	31	32	33

TCM-9000-F09-22

REVISADO - 9 DIC. 2022

COMUNICACIONES Telecomm

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

GEOLOCALIZACIÓN Y DESCRIPCIÓN DEL ENTORNO	Coordenadas Latitud - Longitud:	34	35

Insertar imagen del exterior de la sucursal	Insertar imagen de ventanillas	Insertar imagen del sanitario
36	37	38
Insertar imagen del área de recuento	Insertar imagen de la caja fuerte	Insertar captura de pantalla de la ubicación en Google Maps
39	40	41

42 Agregar Eliminar 43

TCM-9000-F09-22

COMUNICACIONES Telecomm

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

Colindancia:	
Frente a la sucursal:	44
Costado derecho:	45
Costado izquierdo:	46
Espaldas de la sucursal:	47

SEGURIDAD FÍSICA - Características del inmueble					
MATERIALES DE CONSTRUCCIÓN					
Material de construcción de los muros del inmueble:	48	Material de construcción del techo del inmueble:	49	Estacionamiento:	50
Si tiene cortina metálica, indique su ubicación:	51	Material de la puerta del sanitario:	52	Patio:	53
Número de puertas de acceso de la vía pública a la sucursal:	54	Acometida eléctrica:	55	Baño:	56
Total de puertas en la sucursal:	57				

Descripción de la ubicación	Material de la puerta	Número de chapas de la puerta:	Material de la chapa 1:	Material de la chapa 2:	Material de la chapa 3:
58	59	60	61	62	63

TCM-9000-F09-22

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm.

CARACTERÍSTICAS DEL MOSTRADOR					
Material de construcción del mostrador:	64	Número de ventanillas de atención a usuarios:	65	Material de construcción de las ventanillas:	66
La ventanilla cuenta con transfer para documentos:	67	Espacio entre ventanilla y techo (Monzal):	68	Observaciones o comentarios adicionales:	69
CARACTERÍSTICAS DE LAS YENTANAS					
Número de ventanas internas en la sucursal:	70	¿Las ventanas internas tienen protección de herrería?:	71	Observaciones o comentarios adicionales:	72
Número de ventanas externas en la sucursal:	73	¿Las ventanas externas tienen protección de herrería?:	74	Observaciones o comentarios adicionales:	75
EQUIPO ELECTRÓNICO DE SEGURIDAD					
EQUIPO DE VIDEOVIGILANCIA					
Número de cámaras instaladas en la sucursal:	76				
Modelo / Marca	**Ubicación**	**Funciona correctamente**	**Tiene conexión con el Centro Nacional de Monitoreo:**	**Fecha de su ultima revisión**	**Observaciones**
77	78	79	80	81	82

TCM-9000-F09-22

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm.

PANEL DE ALARMA					
Cuenta con panel de alarma:	83	Fecha de la última revisión:	86	Funciona correctamente:	88
La sirena funciona correctamente:	84	Tiene botón de pánico:	87	Funcionan los magnetos de puertas y ventanas:	89
Funcionan los sensores de movimiento:	85	Observaciones:	90		
RESGUARDO DE VALORES					
	SI/NO	**Ubicación**	**Descripción de la seguridad**		
Cofre de seguridad / Tómbola:	91	92	93		
Caja fuerte:	94	95	96		
Área de recuento:	97	98	99		
RESGUARDO POLICIAL					

TCM-9000-F09-22

REVISADO - 9 DIC. 2022

DIRECCIÓN DE LA UNIDAD ESTRATÉGICA DE INTELIGENCIA
SUBDIRECCIÓN DE SEGURIDAD, INVESTIGACIÓN Y SISTEMAS DE PROTECCIÓN
JEFATURA DE ANÁLISIS DE RIESGOS E INTELIGENCIA
FORMATO DE MEDIDAS DE SEGURIDAD EN SUCURSALES

COMUNICACIONES Telecomm

	SÍ/NO	Empresa o corporación	Número de oficio de la Gestión	Número de oficio de respuesta de la autoridad:	Frecuencia del resguardo policial
Vigilancia policial	100	101	102	103	104
Convenio de seguridad con alguna autoridad local	105	106	107	108	109

PROTECCIÓN CIVIL				
	SÍ/NO	Existencia	Localización	Necesidades
Extintores	110	111	112	113
Equipamiento de identificación Protección Civil para el trabajador	114	115	116	117
Señalización	118	119	120	121
Equipo de primeros auxilios	122	123	124	125
UIPC (Unidad Interna de Protección Civil)	126	127	128	129

TCM-9000-F09-22

REVISADO - 9 DIC. 2022

NOMBRE DEL DOCUMENTO:
POLÍTICAS DE SEGURIDAD Y PROTECCIÓN EN SUCURSALES

NÚMERO:
TCM-9000-D03-22

INSTRUCTIVO DE LLENADO DEL FORMATO "MEDIDAS DE SEGURIDAD" TCM-9000-F09-22.

TÍTULO DE LA FORMA:	CLAVE:
FORMATO DE MEDIDAS DE SEGURIDAD	TCM-9000-F09-22

NOMBRE DEL CAMPO	INFORMACIÓN REQUERIDA
1.- Nombre de sucursal	Campo designado para el nombre de la sucursal.
2.- Registro	Seleccionar el número de registro de la sucursal. NOTA: AL SELECCIONAR EL NÚMERO DE SUCURSAL EN AUTOMÁTICO SE DEPLEGARÁN LOS CAMPOS DE: Nombre de sucursal Estado Municipio Localidad
3.- Estado	Campo designado al nombre del Estado de la República dónde se encuentra la sucursal.
4.- Municipio	Campo designado al municipio dónde se localiza la sucursal referida.
5.- Colonia / Localidad	Campo designado al nombre de colonia / localidad dónde se localiza la sucursal referida.
6.- Código postal	Anotar el código postal.
7.- Tipo de sucursal	Seleccionar de las opciones la que corresponda (Unipersonao o multipersonal).
8.- Tipo de población	Seleccionar de las opciones la que corresponda (Rural, semirural o urbano).
9.- Dentro de un espacio público	Seleccionar la opción que corresponda.
10.- Espacio designado	Seleccionar la opción que corresponda.
11.- Tipo de inmueble	Seleccionar el tipo de contrato de arrendamiento del espacio.
12.- Dirección	Anotar el domicilio completo de la ubicación de la sucursal. (Calle, número, colonia, Entidad Federativa, Código Postal).
13.- Valores remesados	Seleccionar la opción que corresponda.
14.- Monto autorizado para el traslado por conducto personal	Anotar el monto autorizado de traslado.
15.- Cantidad de efectivo autorizada para mantener en ventanilla	Anotar la cantidad de efectivo autorizada para mantener en ventanilla.
16.- Cantidad de efectivo autorizada para mantener en caja fuerte	Anota la cantidad de efectivo autorizada para mantener en caja fuerte.
17.- Cantidad sugerida para incremento	Anotar la cantidad sugerida para incremento.
18.- Nivel de riesgo de la localidad	Seleccionar la opción que corresponda.
19.- Reapertura	Selección la opción que corresponda.

REVISADO - 9 DIC. 2022

NOMBRE DEL CAMPO	INFORMACIÓN REQUERIDA
20.- Fecha de reapertura	Describir, sólo sí existe el caso de reapertura.
21.- Motivo de la reapertura	Describir, sólo sí existe el caso de reapertura.
22.- Reubicación	Selección la opción que corresponda.
23.- Fecha de reubicación	Describir, sólo sí existe el caso de reubicación.
24.- Motivo de reubicación	Describir, sólo sí existe el caso de reubicación.
25.- Nombre anterior a la reubicación	Describir, sólo sí existe el caso de reubicación.
26.- Registro anterior a la reubicación	Describir, sólo sí existe el caso de reubicación.
27.- Número de personal adscrito a la sucursal	Seleccionar el número de personal con la que cuenta la sucursal.
28.- Nombre del (de las) servidor (as, es) publico (s)	Escribir el nombre del (de las) servidor (as, es) publico (s) adscritos a la sucursal.
29 .- Puesto que desempeña	Describir las funciones que desempeña cada servidor público.
30 .- Nombre de la plaza que ocupa	Seleccionar el nombre de la plaza de cada servidor público adscrito a la sucursal.
31 .- Nivel	Seleccionar el nivel de la plaza de cada servidor público adscrito a la sucursal.
32.- Código de puesto	Seleccionar el código de puesto de la plaza de cada servidor público adscrito a la sucursal.
33 .- Fecha de ingreso al organismo	Escribir la fecha de ingreso de cada servidor público.
34 .- Latitud	Asentar las coordenadas de ubicación de la sucursal generadas en Google Maps y asentar lo datos referentes a la latitud. 1. Abre Google Maps en tu computadora. 2. Haz clic con el botón derecho en el lugar o en el área del mapa. 3.Se abrirá una ventana emergente. 4. Puedes encontrar tu latitud y longitud en formato decimal en la parte superior. 5. Para copiar las coordenadas automáticamente, haz clic con el botón izquierdo en la latitud y la longitud.
35 .- Longitud	Asentar las coordenadas de ubicación de la sucursal generadas en Google Maps y asentar lo datos referentes a la longitud. 1. Abre Google Maps en tu computadora. 2. Haz clic con el botón derecho en el lugar o en el área del mapa. 3.Se abrirá una ventana emergente. 4. Puedes encontrar tu latitud y longitud en formato decimal en la parte superior. 5. Para copiar las coordenadas automáticamente, haz clic con el botón izquierdo en la latitud y la longitud.

NOMBRE DEL CAMPO	INFORMACIÓN REQUERIDA
42 .- Botón de agregar imágen 43.- Botón de eliminar imágen	36 .- Seleccionar del listado que se despliega del botón "42" de "Agregar" la opción de "Exterior de Sucursal", posteriormente "Insertar imagen" automáticamente de abrirá la carpeta principal del computador, selecciona la carpeta dónde se encuentra guardada la imagen que corresponda a la fotografía del frente de la sucursal, en la que se observe detalladamente el entorno, a fin de que se muestre la estructura del inmueble y los locales que se encuentran a un costado. NOTA: De existir un error de asignación de fotografía, oprimir el campo número 43 "Eliminar imagen" y seleccionar el campo dónde se desea retirar la imagen que no corresponda.
	37.- Seleccionar del listado que se despliega del botón "42" de "Agregar" la opción de "Ventanillas", posteriormente "Insertar imagen" automáticamente de abrirá la carpeta principal del computador, selecciona la carpeta dónde se encuentra guardada la imagen que corresponda a la fotografía que muestre el área de ventanillas y el área de trabajo de los trabajadores. NOTA: De existir un error de asignación de fotografía, oprimir el campo número 43 "Eliminar imagen" y seleccionar el campo dónde se desea retirar la imagen que no corresponda.
	38 .- Seleccionar del listado que se despliega del botón "42" de "Agregar" la opción de "Ambulatorio", posteriormente "Insertar imagen" automáticamente de abrirá la carpeta principal del computador, selecciona la carpeta dónde se encuentra guardada la imagen que corresponda a la fotografía en la que se observe el ambulatorio, en la imagen se deberá apreciar la magnitud de espacio de atención a usuarios. NOTA: De existir un error de asignación de fotografía, oprimir el campo número 43 "Eliminar imagen" y seleccionar el campo dónde se desea retirar la imagen que no corresponda.

REVISADO - 9 DIC. 2022

NOMBRE DEL CAMPO	INFORMACIÓN REQUERIDA
	39 .- Seleccionar del listado que se despliega del botón "42" de "Agregar" la opción de "Área de recuento", posteriormente "Insertar imagen" automáticamente de abrirá la carpeta principal del computador, selecciona la carpeta dónde se encuentra guardada la imagen que corresponda a la fotografía del área de recuento, en dónde se deberá observar la habitación dónde se lleva a cabo el recuento de los recursos.. NOTA: De existir un error de asignación de fotografía, oprimir el campo número 43 "Eliminar imagen" y seleccionar el campo dónde se desea retirar la imagen que no corresponda.
	40 .- Seleccionar del listado que se despliega del botón "42" de "Agregar" la opción de "Caja fuerte", posteriormente "Insertar imagen" automáticamente de abrirá la carpeta principal del computador, selecciona la carpeta dónde se encuentra guardada la imagen que corresponda a la fotografía del área donde se ubica la caja fuerte, de manera que permita visualizar su entorno. NOTA: De existir un error de asignación de fotografía, oprimir el campo número 43 "Eliminar imagen" y seleccionar el campo dónde se desea retirar la imagen que no corresponda.
	41 .- Seleccionar del listado que se despliega del botón "42" de "Agregar" la opción de "Google Maps", posteriormente "Insertar imagen" automáticamente de abrirá la carpeta principal del computador, selecciona la carpeta dónde se encuentra guardada la imagen que corresponda a la fotografía captura de pantalla de la ubicación de la sucursal en Google Maps, en la que deberán considerar aproximadamente dos cuadas a la redonda. NOTA: De existir un error de asignación de fotografía, oprimir el campo número 43 "Eliminar imagen" y seleccionar el campo dónde se desea retirar la imagen que no corresponda.
44 .- Frente a la sucursal	Describir inmuebles y/o lugares que se encuentran frente a la sucursal.
45 .- Costado derecho	Describir inmuebles y/o lugares que se encuentran del lado derecho a la sucursal.
46 .- Costado izquierdo	Describir inmuebles y/o lugares que se encuentran del lado izquierdo de la sucursal.

NOMBRE DEL CAMPO	INFORMACIÓN REQUERIDA
47 .- Espaldas de la sucursal	Describir inmuebles y/o lugares que se encuentran a espaldas de la sucursal.
48 .- Muros	Seleccionar el material de construcción de los muros del inmueble.
49 .- Techos	Seleccionar el material de construcción del techo del inmueble.
50 .- Estacionamiento	Seleccionar la opción que corresponda.
51 .- Cortina	Seleccionar la opción que corresponda.
52 .- Puerta ambulatorio	Seleccionar el material de la puerta del ambulatorio.
53 .- Patio	Seleccionar la opción que corresponda.
54 .- Número de puertas acceso vía pública	Seleccionar el número de puertas acceso vía pública.
55 .- Acometida	Seleccionar la opción que corresponda.
56 .- Baño	Seleccionar la opción que corresponda.
57 .- Total de puertas en sucursal	Seleccionar la opción del total de puertas que corresponda.
58 .- Descripción de la ubicación de la puerta	Seleccionar la opción que corresponda.
59 .- Material de la puerta	Seleccionar la opción que describa el material de la puerta.
60 .- Número de chapas	Seleccionar la opción del número de chapas.
61 .- Material chapa 1	Seleccionar la opción del tipo de chapa.
62 .- Material chapa 2	Seleccionar la opción del tipo de chapa.
63 .- Material chapa 3	Seleccionar la opción del tipo de chapa que corresponda.
64 .- Material del mostrador	Seleccionar la opción del material de construcción del mostrador que corresponda.
65 .- Número de ventanillas	Seleccionar la opción del número de ventanillas con que cuente la sucursal.
66 .- Material de construcción de ventanillas	Seleccionar la opción del material de construcción del material de las ventanillas.
67 .- Ventanilla cuenta con transfer pasa documentos	Seleccionar la opción que corresponda.
68 .- Espacio entre ventanilla y techo (Montel)	Seleccionar la opción que corresponda.
69 .- Observaciones	Describa sólo sí existiese una opción no encontrada.
70 .- Número de ventanas al interior	Seleccionar la opción de número de ventanas al interior de la sucursal que corresponda.
71 .- Protección en ventanas internas	Seleccionar la opción que corresponda.
72 .- Observaciones	Describa sólo sí existiese una opción no encontrada.
73 .- Número de ventanas al exterior	Seleccionar la opción de número de ventanas al exterior de la sucursal que corresponda.

NOMBRE DEL CAMPO	INFORMACIÓN REQUERIDA
74 .- Protección de ventanas al exterior	Seleccionar la opción que corresponda.
75 .- Observaciones	Describa sólo sí existiese una opción no encontrada.
76 .- Número de cámaras	Seleccionar el número de cámaras con que cuenta la sucursal.
77 .- Modelo / Marca de cámara	Seleccionar el modelo / marca de cada una d las cámaras con las que cuenta la sucursal.
78 .- Ubicación de las cámaras	Seleccionar la ubicación de las cámaras con las que cuenta la sucursal.
79 .- Funcionamiento	Seleccionar la opción que corresponda.
80 .- Conexión al CNM	Seleccionar la opción que corresponda.
81 .- Fecha de última revisión	Escribir la última fecha de revisión de las cámaras.
82 .- Observaciones	Describa sólo sí existiese una opción no encontrada.
83 .- Panel de control	Seleccionar la opción que corresponda.
84 .- Sirena	Seleccionar la opción que corresponda.
85 .- Funcionamiento de sensores de movimiento	Seleccionar la opción que corresponda.
86 .- Fecha de última revisión	Escribir la última fecha de revisión del panel de alarma.
87 .- Botón de pánico	Seleccionar la opción que corresponda.
88 .- Funcionamiento del botón de pánico	Seleccionar la opción que corresponda.
89 .- Funcionamiento de magnéticos	Seleccionar la opción que corresponda.
90 .- Observaciones	Describa sólo sí existiese una opción no encontrada.
91 .- Cofre de seguridad	Seleccionar sí existe cofre de seguridad en la sucursal.
92 .- Ubicación del cobre	Seleccionar opción sólo sí se cuenta con cofre de seguridad.
93 .- Descripción del cofre	Seleccionar opción sólo sí se cuenta con cofre de seguridad.
94 .- Caja fuerte	Seleccionar sí existe caja fuerte.
95 .- Ubicación de la caja fuerte	Seleccionar opción sólo sí se cuenta con caja fuerte.
96 .- Descripción de la caja fuerte	Seleccionar opción sólo sí se cuenta con caja fuerte.
97 .- Área de recuento	Seleccionar sí existe área de recuento.
98 .- Ubicación del área de recuento	Seleccionar sí existe área de recuento.
99 .- Descripción de la seguridad del área de recuento	Describir sí existe área de recuento.
100 .- Vigilancia policial	Seleccionar la opción que corresponda.
101 .- Empresa o corporación	Seleccionar detalladamente qué tipo de apoyo, Federal, Estatal, Municipal, etc.
102 .- Número de oficio de gestión	Señalar sí se cuenta con documento de apoyo de elementos de seguridad pública. (Adjuntar como evidencia documental).

NOMBRE DEL CAMPO	INFORMACIÓN REQUERIDA
103 .- Número de oficio de respuesta	Señalar sí se cuenta con documento de apoyo de elementos de seguridad pública. (Adjuntar como evidencia documental).
104 .- Frecuencia del resguardo	Seleccionar la opción que corresponda.
105 .- Convenio de seguridad con alguna autoridad	Seleccionar la opción que corresponda.
106 .- Empresa o corporación	Seleccionar detalladamente qué tipo de apoyo, Federal, Estatal, Municipal, etc.
107 .- Número de oficio de gestión	Señalar sí se cuenta con documento de apoyo de elementos de seguridad pública. (Adjuntar como evidencia documental).
108 .- Número de oficio de respuesta	Señalar si se cuenta con documento de apoyo de elementos de seguridad pública. (Adjuntar como evidencia documental).
109 .-Frecuencia del resguardo	Seleccionar la opción que corresponda.
110 .- Extintores	Seleccionar la opción que corresponda.
111 .- Existencia	Seleccionar la opción que corresponda.
112 .- Localización de extintores	Seleccionar la opción que corresponda.
113 .- Necesidades	Descripción de alguna necesidad en específico.
114 .- Equipo de identificación de Protección Civil	Seleccionar la opción que corresponda.
115 .- Existencia	Seleccionar la opción que corresponda.
116 .- Localización del Equipo de identificación	Seleccionar la opción que corresponda.
117 .- Necesidades del Equipo de identificación	Describir de alguna necesidad en específico.
118 .- Señalización	Seleccionar la opción que corresponda.
119 .- Existencia de señalización	Describir con la señalización con la que se cuenta la sucursal.
120 .- Localización de la señalización	Seleccionar la ubicación de la señalización con la que cuenta la sucursal.
121 .- Necesidades de señalización	Describir de alguna necesidad en específico.
122 .- Equipo de primeros auxilios	Seleccionar la opción que corresponda.
123 .- Existencia de primeros auxilios	Seleccionar la opción que corresponda.
124 . Localización del equipo de primeros auxilios	Seleccionar la opción que corresponda.
125 .- Necesidades de equipo de primeros auxilios	Describir de alguna necesidad en específico.
126 .- Unidad Interna de Protección Civil (UIPC)	Seleccionar la opción que corresponda.
127 .- Existencia (número de integrantes)	Seleccionar la opción que corresponda.
128 .- Localización	N/A
129 .- Necesidades de la UIPC	Describir de alguna necesidad en específico.

REVISADO - 9 DIC. 2022

CONTROL DE ACTUALIZACIONES DEL DOCUMENTO

ACTUALIZACIÓN No. Y FECHA	ELABORARON Y REVISARON:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
Primer Registro ABRIL DE 2015	Gral. José Enrique Ortega Iniestra Enc. de la Subdirección de Diseño y Operación de Sistemas de Protección Gral. Benjamín Rubén Serros Hernández Enc. de la Subdirección de Análisis de Riesgos y Supervisión Mayor Ing. Juan Alfredo Mendoza Castellanos Subdirector de Investigación e Inteligencia Mtro. Daniel Hidalgo Konishi Enc. de la Subdirección de Coordinación Institucional	Gral. José Luis González Arredondo Director de la Unidad Estratégica de Inteligencia	Atender la sugerencia de la Dirección de Asuntos Jurídicos mediante Of. 8001/D/2036, para implementar mecanismos de mejora en las Gerencias Estatales.

NOMBRE DEL DOCUMENTO:
POLÍTICAS DE SEGURIDAD Y PROTECCIÓN EN SUCURSALES

NÚMERO:
TCM-9000-D03-22

ACTUALIZACIÓN No. Y FECHA	ELABORARON Y REVISARON:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
Primera Actualización JULIO DE 2020	Lic. Geovanni Téllez Ávila Subdirector de Seguridad, Investigación y Sistemas de Protección Ing. Alejandro Melo Bravo Gerente de Monitoreo y Videovigilancia	Mtro. Gerardo René Herrera Huízar Director de la Unidad Estratégica de Inteligencia	El presente documento modifica el contenido del anterior TCM-9000-D01-15 (presentación) con número de registro 347 de fecha 15 de abril de 2015, conforme a la modificación al Estatuto Orgánico publicado en el D.O.F. del 14 de febrero de 2018 y aplicación de la nueva Estructura Orgánica del Organismo aprobada y registrada por la Secretaría de la Función Pública mediante los oficios SSFP/408/1091/2018 y SSFP/408/DGOR/1427/2018, con vigencia organizacional a partir del 01 de julio de 2018. 1.- Se incluyó en el capítulo del Plan de Atención a Emergencias, un protocolo en caso de Extorsión. 2.- Se realizaron mejoras a las medidas de seguridad, proponiendo nuevas medidas de control y mejorando las existentes, tomando en cuenta los cambios que enfrenta el Organismo. 3.- Derivado de la modificación del Estatuto Orgánico de Telecomunicaciones de México el 20 de mayo de 2014, se sustituyó el término oficina por sucursal. 4.- Se efectuaron cambios observados por el Órgano Interno de Control en TELECOMM, en la Auditoría N° 3/2016 "Control de Sustracción de Dinero" practicada a la DUEI. 5.- Se actualizaron las características de las cámaras y alarmas. 6.- En el capítulo quinto, Programa de Seguridad y Protección de TELECOMM, punto 2.- Procedimientos preventivos de seguridad, se cambió el orden secuencial de los temas 2.3 y 2.4. 7.- En el capítulo tercero, en el punto 4.1 Traslado de Valores por conducto personal: se modifica su contenido con mejoras en

REVISADO - 9 DIC. 2022

ACTUALIZACIÓN No. Y FECHA	ELABORARON Y REVISARON:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
			caso del traslado de valores por conducto personal en sucursales unipersonales. Para mejora de la política, se hacen cambios en la redacción en todo el numeral. 8.- En el capítulo primero, numeral 7.2.2 Sistema de videovigilancia. Inciso d) Procedimiento para la obtención de imágenes del sistema de videovigilancia. Se modificó el Caso 2. Sistema de videovigilancia IP, respecto a la solicitud de imágenes captadas por los equipos de videovigilancia. 9.- En el capítulo cuarto, numeral 3. Durante el proceso de pago de programas sociales, se agregaron incisos al punto 3.3 y se modificó el punto 3.6, respecto a la recepción de remesas fuera de horario. 10.- En el capítulo cuarto, numeral 4.3 Empresas Trasladadoras de Valores, se modificó el punto 4.3.1, respecto a la responsabilidad de las gerencias estatales de asegurarse de que la empresa que brinde el servicio de traslado de valores cuente con ciertas medidas básicas de seguridad. 11.- En el capítulo tercero, en el punto 4.2 Procesos de coordinación operativa entre la Dirección de la Unidad Estratégica de Inteligencia y las Gerencias Regionales/Estatales, se agregaron dos políticas con el fin de derogar el Procedimiento para el Traslado de Valores por Conducto Personal de sucursal de TELECOMM hacia sucursales bancarias. 12.-Se actualizaron los nuevos términos utilizados por la Reforma Política de la Ciudad de México. 13.-En todo el documento se eliminó la palabra oficinas telegráficas, sustituyendo por el término se sucursales o sucursales de TELECOMM. 14.- Se eliminó la información concerniente al tema de Protección Civil, por ser de

REVISADO - 9 DIC. 2022

ACTUALIZACIÓN No. Y FECHA	ELABORARON Y REVISARON:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
			carácter público, contrario a las presentes Políticas, además de que cada Gerencia Estatal, es responsable de constituir su Unidad Interna de Protección Civil, así como de elaborar e implementar el Programa Interno de Protección Civil, el cual incluyen sus Procedimientos de Actuación para caso de emergencias: Así mismo el coordinador general de la UIPCI/ TELECOMM es el responsable de supervisar que las Gerencias den cumplimiento a lo establecido en su PIPC, así como solicitar y concentrar los requerimientos de información que la Secretaría de Gobernación y SCT solicitan periódicamente al Organismo, por lo anterior se formalizará el Manual para la Elaboración del Programa Interno de Protección Civil y Planes de Emergencia, el cual será difundido entre los Titulares de las Unidades Internas para que sirva como base en su elaboración. 15.- Se hicieron los cambios correspondientes a las observaciones señaladas por el área de Auditoría Interna del OIC, dadas a conocer a la DUEI mediante el Oficio AI/09/437/37/201 de fecha 16 de febrero de 2017 mismas que fueron aceptadas por esta Dirección. 16.-Se consideró favorable utilizar la palabra riesgo de manera cuidadosa conforme al contexto que nos ocupe. 17.- Se actualizó el contenido del FORMATO DE MEDIDAS DE SEGURIDAD TCM-9000-F09-20. 18.-Se agregaron los siguientes términos en el glosario: amago, auditar, gestión de riesgos, oficial de cumplimiento, pagador habilitado, red de sucursales, rondín, supervisor y titular.

REVISADO - 9 DIC. 2022

NOMBRE DEL DOCUMENTO: POLÍTICAS DE SEGURIDAD Y PROTECCIÓN EN SUCURSALES	NÚMERO: TCM-9000-D03-22

ACTUALIZACIÓN No. Y FECHA	ELABORARON Y REVISARON:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
Segunda Actualización diciembre de 2021	Lic. Geovanni Téllez Ávila Subdirector de Seguridad, Investigación y Sistemas de Protección Ing. Alejandro Melo Bravo Gerente de Monitoreo y Videovigilancia	Gral. Div. D. E. M. Edgar Humberto Flores García Director de la Unidad Estratégica de Inteligencia	El presente documento modifica el contenido del anterior TCM-9000-D03-20 con número de registro 415 de fecha 15 de agosto de 2020. Con la finalidad de mejorar las Políticas de Seguridad y Protección en Sucursales aplicables a la operación en la red de sucursales y conforme al oficio 5110.-138/2020 recibido mediante correo electrónico el 28 de octubre de 2020, relativo al Programa Anual de Calidad y Mejora Regulatoria 2021, se realizaron modificaciones de forma a dichas políticas como se detalla a continuación: 1.-Se actualizó el marco jurídico del documento. 2.- Se agregó el primer párrafo en la Introducción. 3.- Se actualizó el formato de medidas de seguridad, en dónde se agregó al apartado de protección civil en el caso de solicitar opinión de la DUEI en materia de seguridad para la apertura o cambio de domicilio de sucursales, adicionalmente, se actualizó el número de formato en todo el documento, quedando el siguiente número TCM-9000-F09-21. 4.- En el apartado de Políticas Generales de Seguridad, se modificó la política número 17. 5.- En el apartado de Políticas Generales de Seguridad, se agregó la política número 18, asimismo, por tanto, cambio el orden secuencial. 6.- En el capítulo III, numeral 1.1. se

REVISADO - 9 DIC. 2022

			eliminaron las palabras "asaltos y robos con" y la palabra "elevadas" se colocó al final del párrafo. 7.- En el numeral 2, del Capítulo III, se modificó el segundo párrafo. 8.- En el numeral 3 del Capítulo III, 5to párrafo se actualizaron los números de teléfono del Centro Nacional de Monitoreo. 9.- Del capítulo IV, numeral 2.2, se modificó el tercer párrafo. 10.- En el numeral 6.2.5.4 del Capítulo I, se agregó una coma, y se eliminó la letra "y". 11.- En el numeral 2.1 del Capítulo III, se agregó la letra "o". 12.- Correcciones ortográficas en todo el documento. 13.- Se modificó el horario de recepción para la emisión de autorización de pernocta de recursos en sucursales en el numeral tres del capítulo tres. 14.-Derivado de las observaciones de la GEN, en numeral 3.1, se sustituyó las palabras "Jefe de Oficina" se sustituyó por "personas responsables de sucursales".

REVISADO - 9 DIC. 2022

NOMBRE DEL DOCUMENTO:
POLÍTICAS DE SEGURIDAD Y PROTECCIÓN EN SUCURSALES

NÚMERO:
TCM-9000-D03-22

ACTUALIZACIÓN No. Y FECHA	ELABORÓ	REVISÓ:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
Tercera Actualización DICIEMBRE DE 2022	Ing. Alejandro Melo Bravo Gerente de Monitoreo y Videovigilancia	Lic. Geovanni Téllez Ávila Subdirector de Seguridad, Investigación y Sistemas de Protección	Lic. Adán García Zamora Director de la Unidad Estratégica de Inteligencia	El presente documento modifica el contenido del anterior TCM-9000-D03-21 con número de registro 440 de fecha 14 de diciembre de 2021. Con la finalidad de mejorar las Políticas de Seguridad y Protección en Sucursales aplicables a la operación en la red de sucursales y conforme al oficio 5000.-357/2021, recibido el 7 de diciembre de 2021, relativo al Programa Anual de Calidad y Mejora Regulatoria 2022, se realizaron modificaciones de forma y de fondo a dichas políticas como se detalla a continuación: 1.- Se corrigió el formato de autorización, colocando al titular de la Subdirección en la revisión y al titular de la Gerencia en la elaboración. 2.-Se actualizó el marco jurídico del documento. 3.- En la Introducción, se modificó el 1er., 4to., 5to., 6to. y 8vo. párrafo, además, el resumen de los apartados del documento. 4.- En el objetivo se cambiaron las palabras "procesos" por "políticas" y "Telecomm" por "TELECOMM". 5.- Se actualizó el formato de medidas de seguridad y se

REVISADO - 9 DIC. 2022

ACTUALIZACIÓN No. Y FECHA	ELABORÓ	REVISÓ:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
				actualizó el número de formato en todo el documento, quedando el siguiente número TCM-9000-F09-22. 6.- En el apartado de Políticas Generales de Seguridad, se corrigió la política número 13. 7.- En el apartado de Políticas Generales de Seguridad, se agregó la política número 20. 8.-Con fundamento en el Artículo 1°, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; el Artículo 13. Principio de presunción de inocencia y Artículo 15. Derecho a la intimidad y a la privacidad, del Código Nacional de Procedimientos Penales, se eliminó el apartado 6.3 EXHIBICIÓN DE FOTOGRAFÍAS Y/O RETRATOS HABLADOS DE PROBABLES RESPONSABLES DE DELITOS A SUCURSALES. 9.- Modificación del numeral 6.2.3, 7.4.3, del Capítulo I. 10.- Actualización de los números telefónicos de Centro Nacional de Monitoreo de la DUEI, en el numeral 7.4.1, del Capítulo I. 11.- Modificación del numeral 7.4.2, del Capítulo I. 14.- En el capítulo IV, numeral

REVISADO -9 DIC. 2022

ACTUALIZACIÓN No. Y FECHA	ELABORÓ	REVISÓ:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
				2.1, tercer párrafo, se cambió la palabra "protección" por "seguridad". 15.- En el capítulo IV, numeral 2.1, se agregó el punto 2.1.1. 16.- En el capítulo IV, numeral 2.3, se agregaron los puntos 2.3.1, 2.3.2, 2.3.3, 2.3.4, 2.3.5 y 2.3.6. 17.- Del capítulo IV, numeral 3, se integró el punto 3.1, se modificó el 6to párrafo y en el último se agregó una dirección de correo electrónico. 18.- Modificación del inciso c, del numeral 4.1.4, del apartado de Traslado de Valores. 19.- Actualización del 3er. párrafo, del numeral 4.1.7, del apartado de Traslado de Valores. 20.-Modificación del numeral 4.2.2, del Capítulo IV. 21.- Se agregó la fracción 3.3, del Capítulo VII. 22.- en todo el documento se cambió la palabra Telecomm por TELECOMM. 23.- En todo el documento se cambió lo siguiente: "Gerente" por "titular de la Gerencia", "Gerentes" por "titulares de las Gerencias" y "Director" por "titular de la Dirección".

REVISADO - 9 DIC. 2022

NOMBRE DEL DOCUMENTO:
POLÍTICAS DE SEGURIDAD Y PROTECCIÓN EN SUCURSALES

NÚMERO:
TCM-9000-D03-22

ACTUALIZACIÓN No. Y FECHA	ELABORÓ	REVISÓ:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
				24.- Se agregaron los siguientes términos al glosario: Intrusión, extorsión, producto de inteligencia, métodos de seguridad, procedimiento, protocolo, sistemas de disuasión, medidas de seguridad, proceso, lineamiento, vigilancia remota, mística de servicio, ostentoso, hermetismo, monitoreo, vehículos motrices, equipo de radiocomunicación, desencriptar, tentativa, Acta Circunstanciada y Acta Administrativa. 25.- Del capítulo VIII, numeral 4.1 y 4.2, se corrigió la fórmula. 26.- Eliminación del Capítulo II. Seguridad Informática en el Manejo de la Información y los Riesgos Asociados con su Incorrecta Protección. Justificación: Con fundamento en el Artículo 27, Fracción XXVII, del Estatuto Orgánico de Telecomunicaciones de México y en las funciones atribuidas a la Gerencia de Seguridad Informática y Comunicaciones, adscrita a la Subdirección de Tecnologías de la Información y Comunicaciones de la Dirección de Administración, en el Manual de Organización Institucional y con base en la sugerencia emitida por la Dirección de la Red de Sucursales, en el FORO del COMERI, durante el periodo del

REVISADO 9 DIC. 2022

ACTUALIZACIÓN No. Y FECHA	ELABORÓ	REVISÓ:	AUTORIZÓ:	MOTIVO DE LA ACTUALIZACIÓN
				7 al 14 de octubre de 2022, en el que se recomendó eliminar el capítulo de referencia, toda vez que ya que existen políticas específicas en la normateca interna del organismo en materia de seguridad informática. En virtud de lo anterior, con objeto de no duplicar las funciones y contravenir documentos normativos en el Organismo, se eliminó el capítulo. 27. Con relación al párrafo anterior, se agregó la Política General número 21. 28.- Derivado de la eliminación de capítulo II, se recorrió el numeral de los capítulos siguientes. 29.- Se sustituyeron Las palabras "Jefe de sucursal o Encargado de sucursal" por "la persona a cargo de la sucursal". 30.- Se agregó el tercer párrafo en el numeral 3.6 del capítulo V. Plan de atención a emergencias. 31.- En el numeral 3.6 del capítulo V. Plan de atención a emergencias, se cambió "Órgano Interno de Control de TELECOMM" por "Órgano Interno de Control en TELECOMM".