SECRETARIA DE HACIENDA Y CREDITO PUBLICO

RESOLUCIÓN que modifica las disposiciones de carácter general aplicables a las instituciones de crédito.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Hacienda y Crédito Público.- Comisión Nacional Bancaria y de Valores.

La Comisión Nacional Bancaria y de Valores, con fundamento en lo dispuesto por los artículos 52, octavo párrafo y 96 Bis de la Ley de Instituciones de Crédito, así como 4, fracciones XXXVI y XXXVIII; 16, fracción I y 19 de la Ley de la Comisión Nacional Bancaria y de Valores, y

CONSIDERANDO

Que en atención al artículo 78 de la Ley General de Mejora Regulatoria y con la finalidad de reducir el costo de cumplimiento de las presentes disposiciones, la Comisión Nacional Bancaria y de Valores, mediante resolución publicada en el Diario Oficial de la Federación el 26 de junio de 2017, reformó la "Resolución modificatoria a las Disposiciones de carácter general aplicables a las instituciones de crédito" publicada en el mismo medio de difusión el 6 de enero de 2017, con el objetivo de ampliar el plazo con el que cuentan las instituciones de crédito para que tengan constituido el 100 % del monto de las estimaciones preventivas para riesgos crediticios que corresponden a las carteras crediticias de consumo no revolvente, hipotecaria de vivienda y microcréditos, conforme a la utilización de la nueva metodología aplicable, al tiempo de precisar cuándo deberán revelar dicha información en sus estados financieros, así como en cualquier comunicado público de información financiera, y

Que a fin de estar en condiciones de hacer frente a riesgos y ataques informáticos que pudieran ocasionar afectaciones a las instituciones de crédito y a la realización de operaciones con los clientes, resulta conveniente fortalecer el marco normativo sobre seguridad de sus sistemas e infraestructuras tecnológicas, así como reforzar los controles internos con los que deberán contar, estableciendo un régimen que procure garantizar la seguridad de la infraestructura tecnológica en que se soportan sus operaciones y la confidencialidad, integridad y disponibilidad de la información, a fin de que cuenten con medidas específicas, tendientes a proteger su información, certeza en su operación y continuidad de los servicios, ha resuelto expedir la siguiente:

RESOLUCIÓN QUE MODIFICA LAS DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE CRÉDITO

ÚNICO.- Se **REFORMAN** los Artículos 1, fracciones XIII, XXXIX y actual fracción LXXXI; 11, primer párrafo; 12, fracción III; 15 Bis, fracción V, primer párrafo; 51 Bis 3, fracción I y último párrafo; 51 Bis 5, fracción I; 51 Bis 9, fracción I; 86, fracción III, inciso b), numerales 1 a 3; 141, fracción III; 160, fracción III; 164, fracción IV, incisos f) y h); 164 Bis, fracción III; 166, fracción III; 169, primer párrafo, 315 Bis, fracción I y 316 Bis 14, primer párrafo; se **ADICIONAN** los Artículos 1, fracciones LXXVI, LXXXIII, CXXXVI, y CXCII, recorriéndose las demás fracciones en su orden y según corresponda; 160, fracción XIV; el Título Segundo, Capítulo VI, Sección Octava Bis a denominarse "De la seguridad de la información" que comprende los artículos 168 Bis 11 a 168 Bis 17; 316 Bis 10, fracción V, así como los Anexos 64 Bis y 72; se **DEROGAN** los Artículos 15 Bis, fracción V, incisos a) a e); 71, fracción IX; 86, fracción III, inciso b), numeral 3, fracciones i. a vi.; 164, fracción V; 166, fracción V; 316 Bis 12; 316 Bis 17 y 316 Bis 20, y se **SUSTITUYEN** los Anexos 64 y 71 de las "Disposiciones de carácter general aplicables a las instituciones de crédito", publicadas en el Diario Oficial de la Federación el 2 de diciembre de 2005, y modificadas mediante resoluciones publicadas en el citado Diario Oficial el 3 y 28 de marzo, 15 de septiembre, 6 y 8 de diciembre de 2006; 12 de enero, 23 de marzo, 26 de abril y 5 de noviembre de 2007; 10 de marzo, 22 de agosto, 19 de septiembre, 14 de octubre y 4 de diciembre de 2008; 27 de abril, 28 de mayo, 11 de junio, 12 de agosto, 16 de octubre, 9 de noviembre, 1 y 24 de diciembre de 2009; 27 de enero, 10 de febrero, 9 y 15 de abril, 17 de mayo, 28 de junio, 29 de julio, 19 de agosto, 9 y 28 de septiembre, 25 de octubre, 26 de noviembre y 20 de diciembre de 2010; 24 y 27 de enero, 4 de marzo, 21 de abril, 5 de julio, 3 y 12 de agosto, 30 de septiembre, 5 y 27 de octubre y 28 de diciembre de 2011; 19 de junio, 5 de julio, 23 de octubre, 28 de noviembre y 13 de diciembre de 2012; 31 de enero, 16 de abril, 3 de mayo, 3 y 24 de junio, 12 de julio, 2 de octubre y 24 de diciembre de 2013; 7 y 31 de enero, 26 de marzo, 12 y 19 de mayo, 3 y 31 de julio, 24 de septiembre, 30 de octubre, 8 y 31 de diciembre de 2014; 9 de enero, 5 de febrero, 30 de abril, 27 de mayo, 23 de junio, 27 de agosto, 21 de septiembre, 29 de octubre, 9 y 13 de noviembre, 16 y 31 de diciembre de 2015; 7 y 28 de abril, 22 de junio, 7 y 29 de julio, 1 de agosto, 19 y 28 de septiembre y 27 de diciembre de 2016; 6 de enero, 4 y 27 de abril, 31 de mayo, 26 de junio, 4 y 24 de julio, 29 de agosto, 6 y 25 de octubre, 18, 26 y 27 de diciembre de 2017; 22 de enero, 14 de marzo, 26 de abril, 11 de mayo, 26 de junio, 23 de julio, 29 de agosto y 15 de noviembre de 2018, para quedar como sigue:

TÍTULOS PRIMERO y **PRIMERO BIS . . .**

TÍTULO SEGUNDO . . .

Capítulos I a **V . . .**

Capítulo VI . . .

Secciones Primera a **Octava . . .**

Sección Octava Bis

De la seguridad de la información

Sección Novena . . .

Capítulos VII a **IX . . .**

TÍTULOS SEGUNDO a **QUINTO . . .**

Anexos 1 a **63 . . .**

Anexo 64 Incidentes de afectación en materia de seguridad de la información.

Anexo 64 Bis Informe de Incidentes de seguridad de la información.

Anexos 65 a **70 . . .**

Anexo 71 Requerimientos técnicos para la captura de huellas dactilares e identificación facial como datos biométricos.

Anexo 72 Indicadores de seguridad de la información.

"Artículo 1.- . . .

I. a XII. **. . .**

XIII. Autenticación: al conjunto de técnicas y procedimientos utilizados para verificar la identidad de:

a) Un Usuario y su facultad para realizar operaciones a través del servicio de Banca Electrónica, o un Usuario de la Infraestructura Tecnológica para acceder, utilizar u operar algún componente de la Infraestructura Tecnológica.

b) Una Institución y su facultad para recibir instrucciones a través del servicio de Banca Electrónica.

XIV. a XXXVIII. **. . .**

XXXIX. Contingencia Operativa: a cualquier evento que dificulte, limite o impida a una Institución a prestar sus servicios o realizar aquellos procesos que pudieran tener una afectación al Público Usuario.

XL. a LXXV. **. . .**

LXXVI. Incidente de Seguridad de la Información: a aquel evento que la Institución evalúe de acuerdo a sus procesos de gestión, que pueda:

a) Poner en peligro la confidencialidad, integridad o disponibilidad de un componente o la totalidad de la Infraestructura Tecnológica utilizada por una Institución o de la información que dicha infraestructura procesa, almacena o transmite.

b) Representar una pérdida, extracción, alteración o extravío de información.

c) Constituir una violación de las políticas y procedimientos de seguridad de la información.

d) Representar la materialización de una pérdida por daños, interrupción, alteración o fallas derivadas del uso del hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de transmisión de información en la prestación de servicios, en Infraestructuras Tecnológicas interconectadas que permiten interacciones entre personas, procesos, datos y componentes de tecnologías de información y telecomunicaciones y que sean causados o deriven, entre otros, en accesos no autorizados, uso indebido de la información o de los sistemas, fraude, robo de información o en interrupción de los servicios, que ponga en riesgo la confidencialidad, integridad y disponibilidad de la información.

e) Vulnerar los sistemas o componentes de la Infraestructura Tecnológica con un efecto adverso para la Institución, sus clientes, terceros, proveedores o contrapartes, comúnmente conocidos como ciber-ataques.

LXXVII. a LXXXI. **. . .**

LXXXII. Información Sensible o Información Sensible del Usuario: a la información del Público Usuario, que contenga nombres, domicilios, teléfonos o direcciones de correo electrónico, o cualquier otro dato que identifique a dichas personas en conjunto con números de tarjetas bancarias, números de cuenta, límites de crédito, saldos, montos y demás datos de naturaleza financiera, así como Identificadores de Usuarios o información de Autenticación.

LXXXIII. Infraestructura Tecnológica: a los equipos de cómputo, instalaciones de procesamiento de datos y comunicaciones, equipos y redes de comunicaciones, sistemas operativos, bases de datos, aplicaciones y sistemas que utilizan las Instituciones para soportar su operación.

LXXXIV. a CXXXV. **. . .**

CXXXVI. Plan Director de Seguridad: al documento que establece la estrategia de seguridad de una Institución para procurar una correcta gestión de la seguridad de la información y evitar la materialización de Incidentes de Seguridad de la Información que podrían afectar de forma negativa a la Institución.

CXXXVII a CLIV. **. . .**

CLV. a CXCI. **. . .**

CXCII. Usuario de la Infraestructura Tecnológica: a la persona, Usuario o componente físico o lógico que acceda, utilice u opere la Infraestructura Tecnológica de las Instituciones.

CXCIII. a CXCVII **. . .”**

“Artículo 11.- Las Instituciones en el desarrollo de la Actividad Crediticia, deberán contar para cada una de las etapas, con procesos, personal adecuado e Infraestructura Tecnológica que permitan el logro de sus objetivos en materia de crédito, ajustándose a las presentes disposiciones, así como a las metodologías, modelos, políticas y procedimientos establecidos en su manual de crédito.

. . .

Artículo 12.- . . .

I. y II. **. . .**

III. Mantener controles adecuados que garanticen la confidencialidad, integridad y disponibilidad de la información que procuren su seguridad tanto física como lógica, así como medidas para la recuperación de la información en casos de Contingencia Operativa, en términos de los Artículos 164 Bis y 168 Bis 11 de estas disposiciones.

IV. **. . .”**

“Artículo 15 Bis.- . . .

I. a IV. **. . .**

V. Mantener la confidencialidad, integridad y disponibilidad de la información observando, en el caso de sistemas administrados por las Instituciones, los controles señalados en el Artículo 168 Bis 11, así como medidas en casos de Contingencia Operativa en términos del Artículo 164 Bis de estas disposiciones.

a) a e) Se derogan.

. . .

. . .”

“Artículo 51 Bis 3.- . . .

I. La descripción detallada del mecanismo, el cual deberá ser aprobado por su Consejo, así como de la Infraestructura Tecnológica empleada en cada parte del proceso.

II. **. . .**

En todo caso, en la implementación del mecanismo aprobado para la conformación de la base de datos de huellas dactilares, las Instituciones deberán primeramente hacer la captura de las huellas dactilares de sus empleados, directivos o funcionarios que tendrán a su cargo recopilar las de los clientes y, posteriormente, recopilarán las de sus clientes. Asimismo, deberán observar lo señalado en los párrafos segundo y tercero de la sección I del Anexo 71 de estas disposiciones”.

"Artículo 51 Bis 5.- . . .

. . .

I. La descripción detallada del proceso, el cual deberá ser aprobado por su Consejo, así como la Infraestructura Tecnológica empleada en cada parte de este.

II. y III. . . .

. . ."

"Artículo 51 Bis 9.- . . .

I. La descripción detallada del proceso, el cual deberá ser aprobado por el Consejo, así como la Infraestructura Tecnológica empleada en cada parte de este.

II. a VII. . . .

. . ."

"Artículo 71.- . . .

I. a VIII. . . .

IX. Aprobar la metodología para clasificar las vulnerabilidades en materia de seguridad de la información de acuerdo a su criticidad, probabilidad de ocurrencia e impacto.

. . ."

"Artículo 86.-. . .

I. y II. . . .

III. . . .

a) . . .

b) . . .

1. Dar cumplimiento a lo que se establece en la Sección Octava Bis del Capítulo VI del Título Segundo de estas disposiciones.

2. Establecer controles para la identificación y resolución de aquellos actos o eventos que puedan generarle a la Institución riesgos derivados de:

   i. La comisión de hechos, actos u operaciones fraudulentas a través de medios tecnológicos.

   ii. El uso inadecuado por parte de los Usuarios de la Infraestructura Tecnológica.

3. Establecer e implementar políticas y procedimientos de clasificación de la información y su tratamiento, de acuerdo con el riesgo que implique que la seguridad de la información sea vulnerada determinado por cada una de las Unidades de Negocio y demás áreas operativas de la Institución. Esta clasificación deberá incluirse en los manuales para la Administración Integral de Riesgos a que se refiere el último párrafo del Artículo 78 de estas disposiciones y utilizarse para evaluar e implementar los controles necesarios en la Infraestructura Tecnológica y en los procesos operativos, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de la Institución y de sus clientes.

   i. a vi. Se derogan.

La Institución deberá evaluar las situaciones que en materia de riesgo tecnológico pudieran afectar su operación ordinaria, las cuales deberán ser vigiladas de manera permanente a fin de verificar el desempeño del proceso de Administración Integral de Riesgos.

c) . . .

. . ."

"Artículo 141.- . . .

I. y II. . . .

III. Los que regulen y controlen lo relativo a la Infraestructura Tecnológica, incluidos los sistemas automatizados de procesamiento de datos y redes de telecomunicaciones a que se refiere el Artículo 52 de la Ley.

IV. . . ."

"Artículo 160.- . . .

. . .

I. y II. . . .

III. Verificar que la Infraestructura Tecnológica que soporta la operación y procesos internos de la Institución, incluyendo los sistemas contables, operacionales de cartera crediticia, con valores o de cualquier otro tipo, cuenten con mecanismos para preservar la integridad, confidencialidad y disponibilidad de la información, que eviten su alteración y cumplan con los objetivos para los cuales fueron implementados o diseñados, en términos del Artículo 168 Bis 11 de estas disposiciones. Asimismo, vigilar periódicamente la Infraestructura Tecnológica a fin de identificar fallas potenciales y verificar que esta genere información suficiente, consistente y que fluya adecuadamente.

. . .

IV. a XIII. . . .

XIV. Evaluar con base en el programa anual de trabajo a que se refiere la fracción XI del presente artículo, el proceso de gestión de Incidentes de Seguridad de la Información al que alude el Artículo 168 Bis 14 de estas disposiciones.

Penúltimo párrafo. - Derogado.

. . ."

"Artículo 164.- . . .

. . .

. . .

I. a III. . . .

IV. . . .

a) a e) . . .

f) Proteger la integridad y adecuado mantenimiento de la Infraestructura Tecnológica, incluidos los sistemas automatizados de procesamiento de datos y redes de telecomunicaciones a que se refiere el Artículo 52 de la Ley, así como la integridad, confidencialidad y disponibilidad de la información recibida, generada, procesada, almacenada y transmitida por estos, en términos del Artículo 168 Bis 11 de las presentes disposiciones. Adicionalmente, se deberán establecer procedimientos para que los clientes puedan reportar el robo o extravío de cualquiera de sus Factores de Autenticación, incluso cuando las Instituciones operen a través de sus comisionistas.

g) . . .

h) Asegurar que se observen procedimientos, estructuras organizacionales y políticas de seguridad de la información acordes con la Institución.

i) . . .

V. Se deroga.

VI. a IX. . . .

. . .

. . .

Artículo 164 Bis.- . . .

. . .

I. y II. . . .

III. Hacer del conocimiento de la Comisión las Contingencias Operativas, mediante correo electrónico remitido a la cuenta contingencias@cnbv.gob.mx, o a través de otros medios que la propia Comisión disponga, debiéndose generar un acuse de recibo electrónico, siempre que estas interrupciones presenten una duración de al menos sesenta minutos y actualicen cualquiera de los siguientes supuestos:

a) Cuando se presenten fallas en la Infraestructura Tecnológica que soporta los servicios de las Sucursales y Banca Electrónica.

b) Cuando generen una afectación en los componentes críticos de la Infraestructura Tecnológica que haya tenido como consecuencia la activación total o parcial del Plan de Continuidad de Negocio.

c) Cuando generen una afectación del 30 % en sus Sucursales; Cajeros Automáticos; Terminales Punto de Venta o puntos de atención de sus comisionistas por escenarios diferentes a afectaciones en la Infraestructura Tecnológica, a los que se refiere el Anexo 67 de estas disposiciones.

La notificación señalada deberá efectuarse dentro de los sesenta minutos siguientes a la actualización de cualquiera de los criterios antes mencionados, debiéndose incluir la fecha y hora de inicio de la Contingencia Operativa; la indicación de si continúa o, en su caso, si ha concluido y su duración; los procesos, sistemas y canales afectados; una descripción del evento que se haya registrado, y una evaluación inicial del impacto o gravedad. La Institución deberá comunicar diariamente a la Comisión, a través de los medios señalados en el primer párrafo de esta fracción, el estado de la Contingencia Operativa hasta en tanto esta no se concluya y, tratándose de la última comunicación, deberá incluir la fecha y hora en que se determine que ha concluido y su duración total.

Asimismo, el director general deberá enviar a la Comisión, en un plazo no mayor a 15 días hábiles posteriores a la conclusión de la Contingencia Operativa, un análisis de las causas que la motivaron, la afectación causada en términos cualitativos y cuantitativos que comprenda, cuando menos, la temporalidad, el impacto monetario desglosando el detalle de los costos, y la indicación de las acciones que se implementarán para minimizar el daño en situaciones similares subsecuentes, incluyendo el plan de trabajo que al efecto se elabore el cual deberá contener al menos el personal responsable de su diseño, implementación, ejecución y seguimiento, plazos para su ejecución, detalle de las actividades realizadas y por realizar, así como los recursos técnicos, materiales y humanos empleados.

. . .”

“Artículo 166.- . . .

I. y II. **. . .**

III. Propicien el correcto funcionamiento de la Infraestructura Tecnológica conforme a las medidas de seguridad a que se refiere el Artículo 168 Bis 11 de las presentes disposiciones, auxiliándose para tal efecto del oficial en jefe de seguridad de la información a que se refiere el Artículo 168 Bis 14 de estas disposiciones, así como la elaboración de información completa, correcta, precisa, íntegra, confiable y oportuna, incluyendo aquella que deba proporcionarse a las autoridades competentes, y que coadyuve a la adecuada toma de decisiones.

IV. **. . .**

V. Se deroga.

Último párrafo.- Derogado.

“Sección Octava Bis

De la seguridad de la información

Artículo 168 Bis 11.- El director general de la Institución será responsable de la implementación del Sistema de Control Interno en materia de seguridad de la información que procure su confidencialidad, integridad y disponibilidad. El marco de gestión a que se refiere este párrafo, deberá asegurar que la Infraestructura Tecnológica, propia o provista por terceros, se apegue a los requerimientos siguientes:

I. Que cada uno de sus componentes realice las funciones para las que fue diseñado, desarrollado o adquirido.

II. Que sus procesos, funcionalidades y configuraciones, incluyendo su metodología de desarrollo o adquisición, así como el registro de sus cambios, actualizaciones y el inventario detallado de cada componente de la Infraestructura Tecnológica, estén documentados.

III. Que se hayan considerado aspectos de seguridad de la información en la definición de proyectos para adquirir o desarrollar cada uno de sus componentes, debiendo incluirlos durante las diversas etapas del ciclo de vida. Este comprenderá la elaboración de requerimientos, diseño, desarrollo o adquisición, pruebas de implementación, pruebas de aceptación por parte de los Usuarios de la Infraestructura Tecnológica, procesos de liberación incluyendo pruebas de vulnerabilidades y análisis de código previos a su puesta en producción, pruebas periódicas, gestión de cambios, reemplazo y destrucción de información.

Tratándose de componentes de comunicaciones y de cómputo, los aspectos de seguridad deberán incluir, al menos, lo siguiente:

a) Segregación lógica, o lógica y física de las diferentes redes en distintos dominios y sub redes, dependiendo de la función que desarrollen o el tipo de datos que se transmitan, incluyendo segregación de los ambientes productivos de los de desarrollo y pruebas, así como componentes de seguridad perimetral y de redes que aseguren que solamente el tráfico autorizado es permitido. En particular, en aquellos segmentos con enlaces al exterior, tales como Internet, proveedores, autoridades, otras redes de la Institución o matriz y otros terceros, todo ello referido a servicios críticos, ya sean sistemas de pagos, equipos de cifrado, autorizadores de operaciones, entre otros, considerar zonas seguras, incluyendo las denominadas zonas desmilitarizadas (DMZ por sus siglas en inglés).

b) Configuración segura de acuerdo con el tipo de componente, considerando al menos, puertos y servicios, permisos otorgados bajo el principio de mínimo privilegio, uso de medios extraíbles de almacenamiento, listas de acceso, actualizaciones del fabricante y reconfiguración de parámetros de fábrica. Se entenderá como principio de mínimo privilegio a la habilitación del acceso únicamente a la información y recursos necesarios para el desarrollo de las funciones propias de cada Usuario de la Infraestructura Tecnológica.

IV. Que cada uno de sus componentes sea probado antes de ser implementado o modificado, utilizando mecanismos de control de calidad que eviten que en dichas pruebas se utilicen datos reales del ambiente de producción, se revele información confidencial o de seguridad, o se introduzca cualquier funcionalidad no reconocida para dicho componente.

V. Que cuente con las licencias o autorizaciones de uso, en su caso.

VI. Que cuente con medidas de seguridad para su protección, así como para el acceso y uso de la información que sea recibida, generada, transmitida, almacenada y procesada en la propia Infraestructura Tecnológica, contando al menos con lo siguiente:

a) Mecanismos de identificación y Autenticación de todos y cada uno de los Usuarios de la Infraestructura Tecnológica, que permitan reconocerlos de forma inequívoca y aseguren el acceso únicamente a las personas autorizadas expresamente para ello, bajo el principio de mínimo privilegio.

Para lo anterior, se deberán incluir controles pertinentes para aquellos Usuarios de la Infraestructura Tecnológica con mayores privilegios, derivados de sus funciones, tales como, la de administración de bases de datos y de sistemas operativos.

Asimismo, se deberán prever políticas y procedimientos para las autorizaciones de accesos por excepción, tales como usuarios de ambientes de desarrollo con acceso a ambientes de producción y con acceso por eventos de contingencia, entre otros. Dichas políticas y procedimientos deberán ser aprobados por el oficial en jefe de seguridad de la información.

b) Cifrado de la información conforme al grado de sensibilidad o clasificación que la Institución determine y establezca en sus políticas, cuando dicha información sea transmitida, intercambiada y comunicada entre componentes, o almacenada en la Infraestructura Tecnológica o se acceda de forma remota.

c) Claves de acceso con características de composición que eviten accesos no autorizados, considerando procesos que aseguren que solo el Usuario de la Infraestructura Tecnológica sea quien las conozca, así como medidas de seguridad, cifrado en su almacenamiento y mecanismos para cambiar las claves de acceso cada 90 días o menos. En el caso de los Usuarios de la Infraestructura Tecnológica asignados a aplicativos o componentes para autenticarse entre ellos, el cambio a que alude este inciso deberá realizarse al menos una vez al año. En el evento de que algún Usuario de la Infraestructura Tecnológica tenga conocimiento de las claves de acceso y deje de prestar sus servicios a la Institución, estas deberán modificarse de manera inmediata.

d) Controles para terminar automáticamente sesiones no atendidas, así como para evitar sesiones simultáneas no permitidas con un mismo identificador de Usuario de la Infraestructura Tecnológica.

e) Mecanismos de seguridad, tanto de acceso físico, como de controles ambientales y de energía eléctrica, que protejan la Infraestructura Tecnológica y permitan la operación conforme a las especificaciones del proveedor, fabricante o desarrollador.

f) Medidas de validación para garantizar la autenticidad de las transacciones ejecutadas por los diferentes componentes de la Infraestructura Tecnológica, considerando, al menos lo siguiente:

1. La veracidad e integridad de la información.

2. La Autenticación entre componentes de la Infraestructura Tecnológica, que aseguren que se ejecutan solo las solicitudes de servicio legítimas desde su origen y hasta su ejecución y registro.

3. Los protocolos de mensajería, comunicaciones y cifrado, los cuales deben procurar la integridad y confidencialidad de la información.

4. La identificación de transacciones atípicas, previendo que las aplicaciones cuenten con medidas de alerta automática para su atención de las áreas operativas correspondientes.

5. La actualización y mantenimiento de certificados digitales y componentes proporcionados por proveedores de servicios que estén integrados al proceso de ejecución de transacciones.

Las medidas a que alude este inciso deberán establecerse acorde con el grado de riesgo que las Instituciones definan para cada tipo de transacción.

VII. Que cuente con mecanismos de respaldo y procedimientos de recuperación de la información que mitiguen el riesgo de interrupción de la operación, en concordancia con lo dispuesto en el Artículo 164 Bis de las presentes disposiciones.

VIII. Que mantenga registros de auditoría íntegros, incluyendo la información detallada de los accesos o intentos de acceso y la operación o actividad efectuada por los Usuarios de la Infraestructura Tecnológica, lo anterior, con independencia del nivel de privilegios con el que estos cuenten para el acceso, generación o modificación de la información que reciban, generen, almacenen o transmitan en cada componente de la Infraestructura Tecnológica, incluyendo actividad de procesos automatizados, así como los procedimientos para la revisión periódica de dichos registros.

Las Instituciones deberán conservar los registros de auditoría a que se refiere esta fracción por un periodo de tres años cuando dichos registros se refieran a actividades realizadas sobre componentes que procesen o almacenen información considerada como crítica de conformidad con la clasificación señalada en el Artículo 86, fracción III, inciso b), numeral 3 de las presentes disposiciones. En caso contrario, el periodo de conservación de los registros será mínimo de seis meses.

IX. Que para la atención de los Incidentes de Seguridad de la Información se cuente con procesos de gestión que aseguren la detección, clasificación, atención y contención, investigación y, en su caso, análisis forense digital, diagnóstico, reporte a niveles jerárquicos competentes, solución, seguimiento y comunicación a autoridades, clientes y contrapartes de dichos incidentes.

Para la detección y respuesta de Incidentes de Seguridad de la Información a que hace referencia el párrafo anterior, el director general deberá designar un equipo que incorpore a personal de las diferentes áreas de la Institución para participar en cada actividad del proceso de gestión antes señalado del que, en todo caso, deberá formar parte el oficial en jefe de seguridad de la información de conformidad con la fracción VII del Artículo 168 Bis 14 de estas disposiciones.

En caso de que se detecte la existencia de vulnerabilidades y deficiencias en la Infraestructura Tecnológica, deberán tomarse las acciones correctivas o controles compensatorios de acuerdo al nivel de riesgo de que se trate, previniendo que los Usuarios de la Infraestructura Tecnológica o la Institución puedan verse afectados.

X. Que sea sometida a la realización de ejercicios de planeación y revisión anuales que permitan medir su capacidad para soportar su operación, garantizando que se atiendan oportunamente las necesidades de incremento de capacidad detectadas como resultado de dichos ejercicios.

Asimismo, la Institución deberá evaluar la obsolescencia de los componentes de la Infraestructura Tecnológica, debiendo contar con un plan para su actualización.

XI. Que cuente con controles automatizados o, en ausencia de estos, que se realicen controles compensatorios, tales como doble verificación, que previo o posteriormente a la realización de la operación de que se trate, minimicen el riesgo de eliminación, exposición, alteración o modificación de información, que se deriven de procesos manuales o semi-automatizados realizados por el personal de la Institución, con el objetivo de prevenir errores, omisiones, sustracción o manipulación de información.

XII. Que tenga controles que permitan detectar la alteración o falsificación de libros, registros y documentos digitales relativos a las operaciones activas, pasivas y de servicios de la Institución.

XIII. Que cuente con procesos para medir y asegurar los niveles de disponibilidad y tiempos de respuesta, que garanticen la ejecución de las operaciones y servicios realizados; lo anterior incluyendo los supuestos en que las Instituciones contraten la prestación de servicios por parte de proveedores externos para el procesamiento y almacenamiento de información.

XIV. Que cuente con dispositivos o mecanismos automatizados para detectar y prevenir eventos e Incidentes de Seguridad de la Información, así como para evitar conexiones y flujos de datos entrantes o salientes no autorizados y fuga de información, considerando entre otros, medios de almacenamiento removibles.

Las Instituciones deberán correlacionar los datos obtenidos de los dispositivos o mecanismos automatizados a que alude el párrafo anterior con los datos de otras fuentes, tales como registros de actividad o de Incidentes de Seguridad de la Información.

Adicionalmente, a lo señalado en el párrafo anterior, las Instituciones deberán mantener controles que eviten la filtración de la información correspondiente a la configuración de la Infraestructura Tecnológica, tales como direcciones IP, reglas de los cortafuegos, así como versiones de hardware y software.

XV. Que para la prestación de servicios de tecnologías de información a los Usuarios de la Infraestructura Tecnológica, en sus fases de estrategia, diseño, transición, operación y mejora continua se proteja la integridad de la Infraestructura Tecnológica así como la integridad, confidencialidad y disponibilidad de la información recibida, generada, procesada, almacenada y transmitida por esta.

El director general será responsable de documentar en políticas y procedimientos lo previsto en este artículo.

Artículo 168 Bis 12.- El director general de la Institución será responsable del cumplimiento de las siguientes obligaciones en relación con la Infraestructura Tecnológica:

I. Aprobar el Plan Director de Seguridad, el cual debe estar alineado con la estrategia de negocio de la Institución, así como definir y priorizar los proyectos en materia de seguridad de la información, con el objetivo de reducir la exposición a los riesgos tecnológicos y la materialización de Incidentes de Seguridad de la Información hasta niveles aceptables en los términos que defina el Consejo, a partir de un análisis de la situación actual.

Para la aprobación de dicho plan, el director general deberá verificar que contenga las iniciativas dirigidas a mejorar los métodos de trabajo existentes y podrá contemplar los controles requeridos conforme a las disposiciones aplicables.

El director general deberá informar al Consejo el contenido del Plan Director de Seguridad, y contar con evidencia de su implementación.

II. Llevar a cabo revisiones de seguridad, enfocadas a verificar la suficiencia en los controles aplicables a la Infraestructura Tecnológica. Estas revisiones deberán comprender al menos lo siguiente:

a) Mecanismos de Autenticación de los Usuarios de la Infraestructura Tecnológica.

b) Configuración y controles de acceso a la Infraestructura Tecnológica.

c) Actualizaciones requeridas para los sistemas operativos y software en general, previo a su implementación y una vez implementados.

d) Identificación de posibles modificaciones no autorizadas al software original.

e) Dispositivos, redes de comunicaciones, sistemas y procesos asociados a los Medios Electrónicos y canales de atención al público, a fin de verificar que no existan vulnerabilidades o se cuente con herramientas o procedimientos que permitan conocer las credenciales de Autenticación de los Usuarios de la Infraestructura Tecnológica, así como cualquier información que de manera directa o indirecta pudiera dar acceso a la Infraestructura Tecnológica en nombre del Usuario de la Infraestructura Tecnológica.

Las revisiones a que se refiere esta fracción deberán realizarse, por lo menos, una vez al año o antes si se presentan cambios significativos en la Infraestructura Tecnológica. Para determinar si se trata de un cambio significativo deberá obtenerse, al efecto, la opinión del oficial en jefe de seguridad de la información.

III. Elaborar un calendario anual para la realización de pruebas de escaneo de vulnerabilidades de los componentes de la Infraestructura Tecnológica que almacenen, procesen o transmitan información, priorizándolos de acuerdo al resultado del ejercicio de clasificación de información a que se refiere el artículo 86, fracción III, inciso b), numeral 3. El calendario deberá prever la revisión trimestral de algunos de los componentes de la Infraestructura Tecnológica de manera que a la conclusión del año se hayan revisado la totalidad de los componentes que almacenen, procesen o transmitan información catalogada como crítica, además de los que la Institución considere necesarios. El director general será responsable de vigilar que dichas pruebas se lleven a cabo ya sea a través de la propia Institución o de un tercero contratado al efecto. Adicionalmente, cuando se incorporen nuevos componentes de la Infraestructura Tecnológica, el director general será responsable de vigilar que se realice la prueba de escaneo de vulnerabilidades, previo a su puesta en producción.

IV. Contratar a un tercero independiente, con personal que cuente con capacidad técnica comprobable mediante certificaciones especializadas de la industria en la materia, para la realización de pruebas de penetración en los diferentes sistemas y aplicativos de la Institución con la finalidad de detectar errores, vulnerabilidades, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información y patrimonio de los clientes y de la propia Institución. Tal revisión deberá incluir la verificación de la integridad de los componentes de hardware y software que permitan detectar alteraciones a estos. Dichas pruebas deberán considerar, al menos lo siguiente:

a) Su alcance y metodología, debiendo ser validados por el oficial en jefe de seguridad de la información.

b) Ser realizadas al menos dos al año sobre sistemas y aplicativos distintos, o bien, cuando lo ordene la Comisión habiendo detectado factores que puedan afectar los sistemas y aplicativos o la información recibida, generada, procesada, almacenada o transmitida en estos. En este último caso, la Comisión determinará el alcance de las pruebas, así como los plazos para realizarlas.

Se podrán efectuar pruebas adicionales a juicio del director general, con opinión del oficial en jefe de seguridad de la información, cuando existan cambios significativos en los sistemas y aplicativos, o realizarlas sobre sistemas y aplicativos previamente revisados cuando existan vulnerabilidades críticas.

El director general de la Institución deberá enviar a la Comisión, dentro de los 20 días hábiles de haber sido finalizadas las pruebas, un informe con las conclusiones de estas. En el envío que se realice, se deberá procurar el uso de mecanismos que impidan el acceso al contenido de este informe por personal no autorizado.

V. Clasificar las vulnerabilidades detectadas de acuerdo con la metodología aprobada por el comité de riesgos.

VI. Elaborar planes de remediación respecto de los hallazgos de las revisiones y pruebas a que se refieren las fracciones II, III y IV anteriores, considerando la clasificación de la fracción V del presente artículo, así como implementar mecanismos de defensa que prevengan el acceso y uso no autorizado de la Infraestructura Tecnológica.

Los planes de remediación a que se refiere el párrafo anterior deberán ser validados por el oficial en jefe de seguridad de la información. Asimismo, dichos planes deberán contener, al menos, la indicación del personal responsable de su implementación y ejecución, así como los plazos para esta, detalle de las actividades realizadas y por realizar, al igual que los recursos técnicos, materiales y humanos empleados. Los referidos planes de remediación deben ser elaborados una vez que se identifiquen las vulnerabilidades y ser enviados a la Comisión en un plazo de 10 días hábiles.

En adición a lo señalado en el párrafo anterior, en caso de tratarse proyectos de corto, mediano o largo plazo en los planes de remediación, deberán incorporarse al Plan Director de Seguridad.

VII. Implementar procesos de seguimiento al cumplimiento de los planes de remediación referidos, lo que deberá ser verificado por el oficial en jefe de seguridad de la información.

VIII. Implementar los programas anuales de capacitación a los que se refiere la fracción V del Artículo 69 de estas disposiciones, así como los de concientización en materia de seguridad de la información, dirigidos a todo el personal y a los clientes incluyendo, en su caso, a terceros que le presten servicios, en los que se contemplen, entre otros aspectos, los roles y responsabilidades que los Usuarios de la Infraestructura Tecnológica tengan al respecto.

IX. Realizar, de manera proactiva e iterativa, la búsqueda de alertas de fraude, así como de amenazas, tales como campañas de correos fraudulentos, sitios de Internet falsos, divulgación de bases de datos con información del Público Usuario, alteración de cajeros automáticos o terminales punto de venta y suplantación de identidad, entre otros, que pudieran afectar a la seguridad de la información del Público Usuario, al igual que acciones para su protección considerando, al menos, lo siguiente:

a) La continua investigación, recopilación, procesamiento y análisis de información que provenga de cualquier fuente relacionada con los productos y servicios que ofrezca la Institución, que pueda constituir indicios o evidencias de que se han evadido los controles de seguridad, representando una amenaza para la información o recursos del Público Usuario.

Los indicios o evidencias a que se refiere el párrafo anterior, se mantendrán en un registro el cual deberá contenerse en la base de datos a que se refiere el primer párrafo del Artículo 168 Bis 17 de estas disposiciones.

b) La implementación de procesos proactivos para proteger la información o recursos de los clientes cuando se presenten los indicios o evidencias señaladas en el inciso a) anterior, tales como bloqueo y reposición de medios de disposición, cambio de datos de autenticación y notificaciones, entre otros.

c) Que cuente con procedimientos de comunicación y recomendaciones de seguridad con los clientes afectados, para informarles sobre los procesos de remediación que la Institución llevará a cabo y, en su caso, las medidas que el propio cliente debe adoptar, tales como cambio de contraseñas, verificación de saldos y movimientos, instalación de antivirus, instalación de software de detección de programas maliciosos, revisión de dispositivos y reinstalación de aplicaciones, entre otros.

Los términos y condiciones para realizar los procesos mediante los cuales se realicen las actividades señaladas en la presente fracción, deberán documentarse en los respectivos manuales de políticas y procedimientos, en los cuales deberá preverse que la Institución mantendrá evidencia de la realización de dichas actividades.

X. Implementar controles que permitan a la Institución asegurar la confidencialidad, integridad y disponibilidad de la información del Público Usuario y de la propia Institución o el acceso a la Infraestructura Tecnológica, por parte de sus empleados o personal que tengan acceso a ella, que garanticen que dicha información e Infraestructura Tecnológica no sean alterados o causen una afectación a la Institución o a los recursos de sus clientes. Dichos controles deberán implementarse desde la contratación respectiva y hasta su terminación.

Artículo 168 Bis 13.- Las Instituciones deberán contar con una persona que se desempeñe como oficial en jefe de seguridad de la información, conocido como CISO por sus siglas en inglés *(Chief Information Security Officer)*.

El oficial en jefe de seguridad de la información deberá ser designado por el director general y ocupar el nivel inmediato inferior al de este debiéndole reportar de manera directa. Será el responsable en materia de seguridad de la información de la Institución y deberá responder a los requerimientos formulados por las autoridades y al interior de la Institución en dicha materia.

El oficial en jefe de seguridad de la información no deberá tener conflictos de interés respecto de áreas de tecnologías de la información, auditoría y Unidades de Negocio dentro de la Institución y no podrá realizar las funciones de las personas encargadas de la implementación y operación de la seguridad de la información de la propia Institución.

Artículo 168 Bis 14.- El oficial en jefe de seguridad de la información de las Instituciones deberá:

I. Participar en la definición y verificar la implementación y continuo cumplimiento de las políticas y procedimientos de seguridad señalados en el Artículo 168 Bis 11 de las presentes disposiciones.

II. Elaborar el Plan Director de Seguridad, el cual deberá contener, por cada proyecto que se defina, nombre del proyecto, objetivo, alcance, fechas de inicio y fin, áreas involucradas y la inversión proyectada. El alcance deberá incluir, entre otros, la magnitud de los trabajos.

III. Verificar al menos anualmente, la definición de los perfiles de acceso a la Infraestructura Tecnológica de la Institución, ya sea propia o provista por terceros, de acuerdo con los perfiles de puestos (segregación funcional), incluyendo aquellos con altos privilegios tales como administración de sistemas operativos, de bases de datos y aplicativos.

IV. Asegurarse al menos anualmente o antes en caso de presentarse un Incidente de Seguridad de la Información de la correcta asignación de los perfiles de acceso a los Usuarios de la Infraestructura Tecnológica. La función a que se refiere esta fracción podrá realizarse mediante muestras representativas y aleatorias.

Asimismo, será responsable de la autorización temporal de los accesos por excepción, tales como los de usuarios de ambientes de desarrollo con acceso a ambientes de producción, accesos por eventos de contingencia o cualquier otro acceso privilegiado que no corresponda con la política determinada por la Institución. Igualmente, deberá contar con un registro que contenga el nombre del Usuario de la Infraestructura Tecnológica, aplicación asociada, ambiente, motivo de la excepción y fecha de inicio y fin de la asignación.

V. Aprobar y verificar el cumplimiento de las medidas que se hayan adoptado para subsanar deficiencias detectadas con motivo de las funciones a que se refieren las fracciones III y IV de este artículo, así como de los hallazgos tanto de auditoría interna como externa relacionada con la Infraestructura Tecnológica y de seguridad de la información.

VI. Gestionar las alertas de seguridad de la información comunicadas por la Comisión u otros medios, así como los Incidentes de Seguridad de la Información, considerando las etapas de identificación, protección, detección, respuesta y recuperación.

VII. Coordinar y presidir en la Institución el equipo para la detección y respuesta de Incidentes de Seguridad de la Información.

VIII. Informar al Comité de Auditoría y al comité de riesgos de la Institución o a los Comités designados para ello, en la sesión inmediata siguiente a la verificación del Incidente de Seguridad de la Información que se trate, respecto de las acciones tomadas y del seguimiento a las medidas para prevenir o evitar que se presenten nuevamente los mencionados incidentes.

IX. Validar la definición de los mecanismos de seguridad mencionados en el Anexo 71 de las presentes disposiciones, así como verificar su cumplimiento.

X. Proponer y coordinar los programas de capacitación y concientización en materia de seguridad de la información dentro de la Institución y hacia el Público Usuario, y verificar su efectividad.

XI. Presentar mensualmente al director general el informe de gestión en materia de seguridad de la información. Este reporte deberá efectuarse a los demás comités o Consejo, según lo determine el director general o a requerimiento de estos.

XII. Tratándose de los indicadores a que se refiere el numeral 7 del inciso a) de la fracción III del artículo 86 de estas disposiciones, en materia de seguridad de la información deberán considerar como indicadores de riesgo al menos los establecidos en el Anexo 72 de estas disposiciones, e informar del resultado de la evaluación de dichos indicadores al Consejo, así como al Comité de Auditoría, comité de riesgos o al comité constituido por la Institución para tales fines.

XIII. Ser el responsable de la implementación de la regulación que en materia de seguridad de la información emitan otras autoridades financieras.

Las Instituciones deberán asegurarse de que el oficial en jefe de seguridad de la información tenga a su disposición los registros de las personas que cuenten con acceso a la información relacionada con las operaciones en las que interviene la propia Institución, incluyendo aquellas que se encuentren en el extranjero y de los Usuarios de la Infraestructura Tecnológica que cuenten con altos privilegios, tales como administración de sistemas operativos y de bases de datos, así como de sus prestadores de servicios.

Las Instituciones que pertenezcan a un grupo financiero sujeto a la supervisión de la Comisión o bien, que formen parte de Consorcios o Grupos Empresariales que cuenten con una entidad financiera sujeta a la supervisión de la propia Comisión, podrán asignar las funciones del oficial en jefe de seguridad de la información, a la persona que desempeñe dichas actividades en la entidad financiera supervisada por la Comisión, siempre y cuando dicha persona cumpla con el Artículo 168 Bis 13 de estas disposiciones.

Artículo 168 Bis 15.- El oficial en jefe de seguridad de la información de las Instituciones podrá apoyarse para el ejercicio de sus funciones en representantes de seguridad de la información de las diferentes Unidades de Negocio denominados oficiales operativos de seguridad de la información, los cuales serán responsables de la aplicación de las políticas y procesos de seguridad de la información en sus respectivas Unidades de Negocio, coadyuvando en los procesos de gestión, reporte de riesgos, evaluaciones de cumplimiento e inteligencia de seguridad.

Dichos oficiales operativos tendrán las siguientes funciones:

I. Verificar la aplicación de las políticas y procedimientos de seguridad de la información en su Unidad de Negocio, debiendo reportar de esta gestión al oficial en jefe de seguridad de la información al menos mensualmente.

II. Reportar al oficial en jefe de seguridad de la información cualquier riesgo o eventualidad que pudiera impactar en la seguridad de la información.

III. Proponer al oficial en jefe de seguridad de la información la adopción de controles de seguridad de la información adicionales.

Los oficiales operativos de seguridad de la información deberán mantenerse actualizados respecto de la normatividad aplicable en dicha materia y podrán recomendar al personal de las Unidades de Negocio la adopción de medidas respecto de la seguridad de la información que previamente hayan sido autorizadas por el oficial en jefe de seguridad de la información.

Artículo 168 Bis 16.- En caso de que se presente un Incidente de Seguridad de la Información que reúna cualquiera de los requisitos a que aluden los incisos a) a d) de la fracción I de este artículo en: (i) los componentes de la Infraestructura Tecnológica de la Institución; (ii) los canales de atención al público, tales como Medios Electrónicos, Oficinas Bancarias o comisionistas de la Institución o, (iii) la infraestructura tecnológica de cualquier tercero que afecte la operación o la Infraestructura Tecnológica de la Institución el director general de la Institución deberá:

I. Prever lo necesario para hacer del conocimiento de la Comisión de forma inmediata los Incidentes de Seguridad de la Información, mediante correo electrónico remitido a la cuenta Ciberseguridad-CNBV@cnbv.gob.mx o a través de otros medios que la propia Comisión señale, debiéndose generar un acuse de recibo electrónico. En dicha notificación se deberá indicar, al menos, la fecha y hora de inicio del Incidente de Seguridad de la Información de que se trate y, en su caso, la indicación de si continúa o, en su caso, si ha concluido y su duración; una descripción de dicho incidente, así como una evaluación inicial del impacto o gravedad.

   Los Incidentes de Seguridad de la Información que deberán reportarse de manera inmediata, serán aquellos que actualicen al menos uno de los siguientes supuestos:

   a) Genere pérdida económica, de información o interrupción de los servicios de la Institución.

   b) Su modo de operación, incluyendo las vulnerabilidades explotadas, pueda replicarse en otras Instituciones.

   c) Pueda representar una afectación a los clientes de las Instituciones, a la estabilidad del sistema financiero o de pagos, o bien, a los sistemas centrales de pagos, a sus prestadores de servicios, cámaras de compensación o a las instituciones para el depósito de valores.

   d) Cualquier otro que se considere grave a juicio de la Institución.

   Adicionalmente, las Instituciones deberán enviar mediante correo electrónico a la Comisión a la cuenta Ciberseguridad-CNBV@cnbv.gob.mx o a través de otros medios que la propia Comisión señale, dentro de los 5 días hábiles siguientes a la identificación del Incidente de Seguridad de la Información de que se trate, la información que se contiene en los Anexos 64 y 64 Bis de las presentes disposiciones.

   Las Instituciones deberán conservar y mantener a disposición de la Comisión, por el período señalado en el artículo 168 Bis 17 de estas disposiciones, los registros de los Incidentes de Seguridad de la Información que no reúnan ninguna de las características aludidas en los incisos anteriores.

II. Llevar a cabo una investigación inmediata sobre las causas que generaron el Incidente de Seguridad de la Información y establecer un plan de trabajo que describa las acciones a implementar para eliminar o mitigar los riesgos y vulnerabilidades que propiciaron el mencionado incidente. Dicho plan deberá indicar, al menos, el personal responsable de su diseño, implementación, ejecución y seguimiento, plazos para su ejecución, así como los recursos técnicos, materiales y humanos, y enviarse a la Comisión en un plazo no mayor a 15 días hábiles posteriores a que concluyó el Incidente de Seguridad de la Información.

Cuando el Incidente de Seguridad de la Información refiera a que la Información Sensible que se encuentre en custodia de la Institución o de terceros que le presten servicios, fue extraída, extraviada, eliminada, alterada o bien, las Instituciones sospechen de la realización de algún acto que involucre accesos no autorizados a dicha información, el director general o la persona que este designe, deberán notificar a los clientes la posible pérdida, extracción, alteración, extravío o acceso no autorizado a su información, dentro de las siguientes 48 horas a que ocurrió el Incidente de Seguridad de la Información o a que se tuvo conocimiento de este, a través de los medios de notificación que el cliente haya señalado para tal efecto, a fin de prevenirlo de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada, eliminada, o alterada, debiendo informarle las medidas que deberá tomar y, en su caso, efectuar la reposición de los medios de disposición que correspondan o la sustitución de Factores de Autenticación necesarios. La evidencia de esta notificación deberá incluirse en el resultado de la investigación señalada en el párrafo anterior.

Artículo 168 Bis 17.- Las Instituciones deberán llevar un registro en bases de datos, de los incidentes, fallas o vulnerabilidades detectadas en la Infraestructura Tecnológica, que incluya al menos la información relacionada con la detección de fallas, errores operativos, intentos de ataques informáticos y de aquellos efectivamente llevados a cabo así como de pérdida, extracción, alteración, extravío o uso indebido de información de los Usuarios de la Infraestructura Tecnológica, en donde se contemple la fecha del suceso y una breve descripción de este, su duración, servicio o canal afectado, clientes afectados y montos, así como las medidas correctivas implementadas.

La información a que se refiere el presente artículo deberá estar respaldada en los medios que las Instituciones determinen y conservarse por, al menos, 10 años."

"Artículo 169.- Las Instituciones deberán documentar en manuales, las políticas y procedimientos relativos a las operaciones propias de su objeto, incluyendo los relativos al funcionamiento de su Infraestructura Tecnológica, los cuales deberán guardar congruencia con los objetivos y lineamientos del Sistema de Control Interno, así como describir las funciones de Contraloría Interna de la Institución.

. . ."

"Artículo 315 Bis.- . . .

I. Los clientes ordenantes deberán registrar las instrucciones para el pago de la orden indicando los datos de los beneficiarios, incluyendo nombre completo, fecha de nacimiento y número de línea de Teléfono Móvil. Asimismo, deberá señalarse el monto individualizado asignado a cada uno de ellos, el cual no podrá exceder del equivalente en moneda nacional a las Operaciones Monetarias de Mediana Cuantía.

II. a V. **. . .**

. . ."

"Artículo 316 Bis 10.- . . .

I. a IV. **. . .**

V. Tratándose del servicio de Banca Electrónica en el que se utilicen tarjetas de débito y de crédito, con las certificaciones que se indican a continuación:

a) Certificaciones de normas de seguridad de la industria de tarjetas, incluyendo entre otras: la norma de seguridad de datos (PCI-DSS), la norma de seguridad de datos para las aplicaciones de pago (PA-DSS) y los requisitos de seguridad y transacciones con NIP (PTS) o sus equivalentes o aquellos que, a criterio de la Comisión, permitan la debida protección de la información almacenada, transmitida o procesada.

b) Certificación conforme al estándar de interoperabilidad de tarjetas de débito y de crédito conocido como EMV, niveles 1 (interfaces, físico, eléctrico y de transporte) y 2 (selección de aplicaciones de pago y procesamiento de transacciones), en su caso, aquellos otros estándares que, a criterio de la Comisión, satisfagan este requerimiento y permitan la adecuada interoperabilidad. Lo anterior solo aplicará en aquellos Dispositivos de Acceso para operaciones con Tarjeta Bancaria con Circuito Integrado en que la información para realizar operaciones se toma directamente del circuito integrado de esta."

"Artículo 316 Bis 12.- Se deroga."

"Artículo 316 Bis 14.- Las Instituciones deberán mantener en bases de datos todas las operaciones efectuadas a través del servicio de Banca Electrónica que no sean reconocidas por sus Usuarios y que, al menos, incluya la información relacionada con operaciones no reconocidas por los Usuarios y el trámite que, en su caso, haya promovido el Usuario, tales como folio de reclamación, fecha de reclamación, causa o

motivo de la reclamación, fecha de la operación, cuenta origen, tipo de producto, servicio de Banca Electrónica en el que se realizó la operación, importe, estado de la reclamación, resolución, fecha de resolución, monto abonado, monto recuperado y monto quebrantado.

. . .”

“Artículo 316 Bis 17.- Se deroga.”

“Artículo 316 Bis 20.- Se deroga.”

TRANSITORIOS

PRIMERO.- La presente Resolución entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación, salvo por lo dispuesto en los artículos transitorios siguientes.

SEGUNDO.- Las normas contenidas en el artículo 86, fracción III, inciso b), numeral 3, que se reforma y 168 Bis 11 fracciones II, III inciso b), IV, VI, incisos b) a e), IX, XIV último párrafo; 168 Bis 12 fracciones II, III, VIII y 168 Bis 14, fracción VI, que se adicionan con esta Resolución, entrarán en vigor a los seis meses siguientes al de su publicación en el Diario Oficial de la Federación.

Las obligaciones del artículo 168 Bis 11, en relación con los requerimientos de la infraestructura tecnológica, según dicho término se define en esta Resolución, que sea provista por terceros que hayan sido contratados por las instituciones de crédito con anterioridad a la entrada en vigor de este instrumento, deberán cumplirse en un plazo máximo de tres años contados a partir de la entrada en vigor de esta Resolución o bien, al momento de la renovación de la contratación respectiva, lo que ocurra primero. Las contrataciones con terceros realizadas por las instituciones de crédito para la provisión de la infraestructura tecnológica, que sean contratadas a partir del inicio de vigencia de esta Resolución, deberán ajustarse a los requerimientos del artículo 168 Bis 11, a los seis meses contados a partir de la entrada en vigor de este instrumento.

TERCERO.- Las obligaciones contenidas en los artículos 168 Bis 11 fracciones VI, inciso a), X, XIII, XV; 168 Bis 12 fracciones I, V; 168 Bis 13; 168 Bis 14 fracciones I, II, IV segundo párrafo, VII, VIII, XI, XII, XIII y segundo párrafo de dicho artículo, que se adicionan con esta Resolución, entrarán en vigor a los nueve meses siguientes al de su publicación en el Diario Oficial de la Federación.

Las instituciones a que se refiere el artículo 2, fracción II, de la Ley de Instituciones de Crédito, deberán hacer la designación a que alude el artículo 168 Bis 13, a los doce meses siguientes al de su publicación en el Diario Oficial de la Federación.

Hasta en tanto no se lleve a cabo la designación de la persona señalada en el artículo 168 Bis 13 de esta Resolución, las instituciones de crédito estarán obligadas a llevar a cabo las funciones respectivas, a través de la persona que, a la entrada en vigor de esta Resolución, se encuentre a cargo de la vigilancia de la seguridad de la información.

CUARTO.- Las obligaciones contenidas en los artículos 168 Bis 11 fracciones VI, inciso f), VIII, XI, XII, XIV primer y segundo párrafos; 168 Bis 12 fracciones IV, VI, VII, IX y X; 168 Bis 14 fracciones III, IV primer párrafo, V, IX, X; así como del 316 Bis 10, fracción V respecto de los comercios y para las propias instituciones preverse en el plan director de seguridad, según dicho término se define en esta Resolución, que se adicionan, entrarán en vigor a los doce meses siguientes al de su publicación en el Diario Oficial de la Federación.

QUINTO.- La obligación contenida en el artículo 168 Bis 11, fracción III, inciso a), que se adiciona con esta Resolución, entrará en vigor a los dieciocho meses siguientes al de su publicación en el Diario Oficial de la Federación.

SEXTO.- Las normas contenidas en los artículos 15 Bis, fracción VI, inciso c); 164, fracción VI, incisos b) y c); y 316 Bis 17, quedarán derogadas a los seis meses siguientes al de la publicación en el Diario Oficial de la Federación de esta Resolución.

SÉPTIMO.- Las normas contenidas en los artículos 15 Bis, fracción V, inciso a) y 166, fracción V, quedarán derogadas a los nueve meses siguientes al de la publicación en el Diario Oficial de la Federación de la presente Resolución.

OCTAVO.- Las normas contenidas en los artículos 15 Bis, fracción V, inciso d), 164, fracción V, incisos g) y h) y 316 Bis 20, quedarán derogadas a los doce meses siguientes al de la publicación en el Diario Oficial de la Federación de la presente Resolución.

Atentamente

Ciudad de México, 15 de noviembre de 2018.- El Presidente de la Comisión Nacional Bancaria y de Valores, **José Bernardo González Rosas**.- Rúbrica.

ANEXO 64

Incidentes de afectación en materia de seguridad de la información

I. Información de la Institución

a) Nombre de la Institución.

b) Nombre completo del oficial en jefe de seguridad de la información, así como su número de teléfono y dirección de correo electrónico.

II. Información detallada del Incidente de Seguridad de la Información

Descripción del Incidente de Seguridad de la Información		
a)	Fecha y hora en que ocurrió	
b)	Fecha y hora en que se detectó	
c)	Duración del incidente	
d)	Ubicación de la instalación afectada (centro de datos, Oficina Bancaria)	
e)	¿La información involucrada en el incidente es administrada por terceros?	Si ( ) No ( )
f)	En caso de ser afirmativo el inciso e), detallar datos del proveedor (nombre, dirección y datos de contacto, correo electrónico, teléfono, entre otros)	

Afectación provocada por el Incidente de Seguridad		
g)	¿El incidente puede ocasionar una pérdida monetaria para los clientes o para la propia institución?	Si ( ) No ( )
h)	¿Es viable recuperar de manera directa (gestiones propias) o indirecta (a través de seguros) la posible pérdida monetaria, a través de otras instituciones o entidades financieras?	Si ( ) No ( )
i)	¿Se han identificado otros incidentes relacionados con el que se reporta, sea por origen, modo de operación o afectación?	Si ( ) No ( )

j) Indicar, en su caso, el tipo de información comprometida con el Incidente de Seguridad de la Información, conforme a las tablas siguientes:

Información personal del cliente comprometida		
Nombres	Si ( )	No ( )
Domicilios	Si ( )	No ( )
Números de teléfono	Si ( )	No ( )
Direcciones de correo electrónico	Si ( )	No ( )
Datos biométricos (huellas dactilares, patrones en iris o retina o reconocimiento facial, entre otros)	Si ( )	No ( )
Otro(s):		

Información de cuentas o saldos		
Números de tarjetas de débito, crédito u otras	Si ( )	No ( )
Números de cuenta	Si ( )	No ( )
Contraseñas o números de identificación personal	Si ( )	No ( )
Identificadores de usuarios	Si ( )	No ( )
Límites de crédito	Si ( )	No ( )
Saldos	Si ( )	No ( )
Otro(s)		

Información de la Institución	
Claves de acceso	Si ( ) No ( )
Configuraciones de seguridad	Si ( ) No ( )
Identificación de puertos o servicios	Si ( ) No ( )
Direcciones IP de componentes o servicios	Si ( ) No ( )
Direcciones IP de componentes internos	Si ( ) No ( )
Acceso a segmentos internos de red	Si ( ) No ( )
Versiones de software, sistemas operativos o bases de datos	Si ( ) No ( )
Identificación de vulnerabilidades	Si ( ) No ( )
Otro(s)	

III. Clasificar el Incidente de Seguridad de la Información reportado con base en las siguientes definiciones:

Clase de Incidentes de Seguridad de la Información	
a) Ataques físicos	
Sabotaje	Si ( ) No ( )
Vandalismo	Si ( ) No ( )
Robo de dispositivos	Si ( ) No ( )
Fuga de información en medios físicos	Si ( ) No ( )
Accesos físicos no autorizados	Si ( ) No ( )
Coerción	Si ( ) No ( )
Extorsión	Si ( ) No ( )
Ataque terrorista	Si ( ) No ( )
Otro(s):	
b) Daño no intencional o accidental, pérdida de información o pérdida de activos	
Información compartida indebidamente	Si ( ) No ( )
Errores u omisiones en sistemas o dispositivos	Si ( ) No ( )
Errores en procedimientos o controles	Si ( ) No ( )
Cambios indebidos a datos	Si ( ) No ( )
Extravío de información o dispositivos	Si ( ) No ( )
Otro(s):	
c) Incidentes por desastres naturales o ambientales	
Terremotos	Si ( ) No ( )
Inundaciones	Si ( ) No ( )
Huracanes	Si ( ) No ( )
Incendios	Si ( ) No ( )
Radiaciones	Si ( ) No ( )
Corrosiones	Si ( ) No ( )
Explosiones	Si ( ) No ( )
Otro(s):	

d) Incidentes por fallas o mal funcionamiento	
Dispositivos	Si ( ) No ( )
Sistemas	Si ( ) No ( )
Comunicaciones	Si ( ) No ( )
Servicios	Si ( ) No ( )
Equipos de terceros	Si ( ) No ( )
Cadena de suministros	Si ( ) No ( )
Otro(s):	
e) Incidentes por la interrupción o falta de insumos	
Ausencia de personal	Si ( ) No ( )
Huelgas	Si ( ) No ( )
Energía	Si ( ) No ( )
Agua	Si ( ) No ( )
Telecomunicaciones	Si ( ) No ( )
Otro(s):	
f) Incidentes por intercepción de datos	
Espionaje	Si ( ) No ( )
Mensajes	Si ( ) No ( )
Wardriving	Si ( ) No ( )
Ataques de hombre en medio	Si ( ) No ( )
Secuestro de sesiones	Si ( ) No ( )
Sniffers	Si ( ) No ( )
Robo de mensajería	Si ( ) No ( )
Otro(s):	
g) Incidentes por actividad maliciosa con el fin de tomar el control, desestabilizar o dañar un sistema informático	
Robo de identidad	Si ( ) No ( )
Phishing	Si ( ) No ( )
Denegación de servicios (DOS, DDOS)	Si ( ) No ( )
Código malicioso (malware, troyanos, gusanos, inyección de código, virus, ransomware)	Si ( ) No ( )
Ingeniería social	Si ( ) No ( )
Vulneración de certificados (suplantación de sitios, certificados falsos)	Si ( ) No ( )
Manipulación de hardware (proxies anónimos, skimmers, instalación de sniffers)	Si ( ) No ( )
Alteración de información (suplantación de direccionamiento y tablas de ruteo, DNS poisoning, alteración de configuraciones)	Si ( ) No ( )
Abuso de herramientas de revisión de seguridad de la información	Si ( ) No ( )
Ataques de fuerza bruta	Si ( ) No ( )
Abuso de autorizaciones	Si ( ) No ( )
Crimen organizado	Si ( ) No ( )

Hacktivistas	Si ( )	No ( )
Gobierno o grupos afines	Si ( )	No ( )
Terroristas	Si ( )	No ( )
Insiders	Si ( )	No ( )
Otro(s):		
h) Incidentes originados por aspectos legales		
Violación de cláusulas contractuales	Si ( )	No ( )
Violación de acuerdos de confidencialidad	Si ( )	No ( )
Decisiones adversas (resoluciones judiciales en la misma jurisdicción o en otras)	Si ( )	No ( )
Otro(s):		
i) Otros (especificar)		

IV. Señalar en las tablas siguientes la clasificación en las que se ubica el incidente mediante los conceptos del catálogo siguiente:

Especificar en cuál de las siguientes categorías se ubica el incidente:

Catálogo del tipo de incidente		
Clave	Tipo	
1	Ciberseguridad	( )
2	Suplantación de Identidad	( )
3	Asalto/Robo	( )
4	Intrusión física	( )
5	Pérdida de información	( )
999	Otro	( )

Indicar la(s) línea(s) de negocio afectadas por el incidente:

Catálogo de líneas de negocio		
Clave	Producto	
101	Créditos Comerciales	( )
102	Créditos de Consumo	( )
103	Créditos a la Vivienda	( )
104	Tarjetas de Crédito	( )
105	Divisas	( )
106	Derivados	( )
107	Reportos	( )
108	SPEI/SPID/SWIFT	( )
109	Valores e Instrumentos de Inversión	( )
110	Cuentas de ahorro, vista, etc.	( )
112	Productos no Bancarios	( )
199	Otro	( )

Indicar los canales afectados por el incidente:

Catálogo de canal afectado		
Clave	Canal	
201	Operaciones por Internet Personas Físicas	( )
202	Operaciones por Internet Personas Morales	( )
203	Comercio por Internet	( )
204	Banca por Teléfono	( )
205	Comercio por Teléfono	( )
206	Cajeros Automáticos	( )
207	Terminal Punto de Venta	( )
208	Sucursales	( )
209	Corresponsales	( )
210	Pago Móvil	( )
211	Banca Móvil	( )
212	Movimiento generado por el Banco	( )
213	Otros Bancos	( )
299	Otro	( )

Indicar el tipo de activo afectado por el incidente:

Catálogo de activo afectado		
Clave	Activo impactado	
301	Estados de Cuenta	( )
302	Plásticos de tarjetas	( )
303	Chequeras	( )
304	NIP´s	( )
305	Contraseñas	( )
306	Bases de Datos	( )
307	TOKEN	( )
399	Otro	( )

Nombre y firma del oficial en jefe de seguridad de la información

ANEXO 64 Bis

Informe de Incidentes de Seguridad de la Información

I. Información de la Institución

a) Nombre de la Institución.

b) Nombre completo del oficial en jefe de seguridad de la información, así como su número de teléfono y dirección de correo electrónico.

II. Información detallada del Incidente de Seguridad de la Información

a) Anexar en medio digital cifrado la siguiente información:

1. Descripción del Incidente de Seguridad de la Información.
2. Números de cuenta afectadas.
3. Estado de las cuentas afectadas (bloqueada, suspendida, activa).
4. Zona de red afectada (internet, red interna, red de administración, entre otras).
5. Tipo de sistema afectado (servidor de archivos, servidor web, servicio de correo, base de datos, estaciones de trabajo, ya sea de escritorio o móvil, entre otros).
6. Sistema operativo (especificar versión).
7. Protocolos o servicios de los componentes impactados.
8. Número de componentes de los sistemas de la Institución afectados.
9. Aplicaciones involucradas (especificar versión).
10. Información del dispositivo comprometido, en su caso (marca, versión de software, firmware, entre otros).
11. Impacto al servicio (considerando cualquier disrupción) ocasionado por el Incidente de Seguridad de la Información.
12. Monto de la pérdida en pesos, en su caso.
13. Monto recuperado en pesos, en su caso.
14. Estado del Incidente de Seguridad de la información (Resuelto o No Resuelto).
15. Señalar si el Incidente de Seguridad de la información se ha dado a conocer a alguna autoridad. En caso afirmativo, indicar la autoridad y la fecha.
16. Direcciones IP públicas, direcciones de correo electrónico o dominios de dónde proviene el ataque.
17. El protocolo de comunicación utilizado, en su caso.
18. La URL en caso de sitios web involucrados.
19. El malware o firma detectada.
20. Detallar las acciones que se realizaron para mitigar el Incidente de Seguridad de la información, mencionando las personas responsables de implementar dichas acciones de mitigación.
21. Descripción de los resultados de las acciones de mitigación.
22. Acciones para minimizar el daño en situaciones similares subsecuentes.
23. Otra información que considere deba ser de conocimiento de esta Comisión.

_____

Nombre y firma del oficial en jefe de seguridad de la información

ANEXO 71

REQUERIMIENTOS TÉCNICOS PARA LA CAPTURA DE HUELLAS DACTILARES E IDENTIFICACIÓN FACIAL COMO DATOS BIOMÉTRICOS

I. Captura de huella dactilar

Los registros de huellas dactilares que realicen las Instituciones consistirán en una toma de imagen de las crestas papilares de los dedos sobre una superficie de contraste por presión, a partir de la cual se obtienen los datos biométricos. Dicha toma deberá considerar controles que aseguren que se obtienen directamente de la persona, evitando el registro de huellas provenientes de impresiones en algún material que pretenda simular la huella de otra persona (prueba de huella viva).

El proceso de primera captura de huellas dactilares deberá consistir en registrar, en primer lugar, las diez huellas dactilares de los empleados, directivos y funcionarios de las Instituciones que estarán a cargo de registrar las huellas de los clientes. En segundo lugar, los referidos empleados, directivos y funcionarios referidos, procederán a capturar al menos, seis huellas dactilares de los clientes de la Institución. Para lo anterior, las Instituciones deberán auxiliarse del o los responsables de las funciones de Contraloría Interna para que se verifique lo previsto en este párrafo.

El proceso de captura de huellas dactilares deberá impedir que un empleado, directivo o funcionario de la Institución registre sus propias huellas dactilares en sustitución de las del cliente. Las Instituciones en todo momento deberán garantizar la integridad de la información biométrica almacenada o trasmitida, así como la conservación, disponibilidad y la imposibilidad de manipulación de tal información. Para efectos de lo previsto en este párrafo las Instituciones deberán ajustarse al menos a lo siguiente:

a) Segregar lógica y físicamente la Infraestructura Tecnológica en que se mantienen las bases de datos de información biométrica, incluyendo la segmentación de las diferentes redes involucradas.

b) Configurar de manera segura los equipos, de acuerdo al tipo de elemento de Infraestructura Tecnológica, puertos, servicios, permisos, listas de acceso, actualizaciones del fabricante y configuración de fábrica.

c) Establecer controles de acceso y mecanismos de identificación y autenticación de todos y cada uno de los Usuarios de la Infraestructura Tecnológica, que permitan reconocerlos de forma inequívoca y aseguren el acceso únicamente a las personas autorizadas expresamente para ello. Ambos mecanismos deberán incluir controles específicos para aquellos Usuarios de la Infraestructura Tecnológica con mayores privilegios, derivados de sus funciones, tales como las de administración de bases de datos y de sistemas operativos, incluyendo registros de auditoría sobre todos los accesos.

d) Contar con mecanismos de cifrado de la información cuando sea transmitida o almacenada.

e) Realizar pruebas tendientes a detectar vulnerabilidades y amenazas, así como de penetración en los diferentes elementos de la Infraestructura Tecnológica a fin de implementar mecanismos de defensa que prevengan el acceso y uso no autorizado de la información.

f) Implementar controles para la conservación de la información, incluyendo aquellos respecto de la integridad de la información almacenada, que permitan identificar cualquier cambio a los datos originales, así como de conservación y borrado seguro que eviten en todo momento que puedan ser conocidos por terceros no autorizados.

Las Instituciones deberán utilizar lectores de huellas de al menos dos dedos por lectura (dispositivos duales) para el procedimiento de primera captura de huellas dactilares para la integración de sus bases de datos.

Para el proceso de captura de huellas dactilares, los requerimientos mínimos de la imagen son los siguientes:

Resolución del escáner (puntos por pulgada)	Profundidad (pixeles)	Rango dinámico mínimo (niveles de gris)
500	8 bits	200

Parámetros de operación de la plataforma (software y hardware) para la captura de huellas dactilares

Las aplicaciones y dispositivos utilizados en el proceso de captura de huellas dactilares en una superficie de contraste por presión, con el fin de integrar una base de datos con tal información, deberán considerar al menos los siguientes requerimientos:

PARÁMETRO	DECISIÓN	OBSERVACIÓN
Primera captura de huellas dactilares		
Imagen capturada		
Tipo de toma	M	Plana en vivo.
Número de dedos	M	De 10 para empleados, directivos y funcionarios. De 6 para clientes como mínimo. Lo anterior, salvo la excepción que se establece en este anexo.
Posición de los dedos	MP	Los dedos deberán ser colocados en el centro del plato con respecto al horizonte de este y paralelos a la superficie de captura.
Ángulo de captura	MP	Los dedos deberán ser colocados a 90° con una rotación de ±10° con respecto al horizonte del plato.
Movimiento en la captura	MP	Evitar el deslizamiento de las huellas sobre el plato al momento de realizar la captura, para evitar imágenes manchadas.
Visualización	MP	El operador debe observar en tiempo real información de la captura.
Segmentación	MP	Probado por el NIST en la prueba denominada “Slap Seg II test”.
Secuencia	M	Validar que no se repitan las huellas de cada dedo durante un mismo proceso de captura.
Deduplicación	M	Validar que las huellas de los clientes o empleados de la Institución no se encuentren previamente registradas en la base de datos con la información de otro cliente o empleado de la Institución.
Dispositivos		
Dual	M	Certificados EFTS anexo F FAP 45.
Decadactilares (4-4-2)	M	Certificados EFTS anexo F FAP 60. Revisión de secuencia.
Imagen	M	Genera RAW. Vista previa de la toma realizada.
Información a obtener del dispositivo	M	El número de serie es obligatorio. Opcionalmente el dispositivo debe tener versión de Firmware, fabricante, y modelo.
Operación		
Asistido	M	Sí. Captura de huellas jerárquica y se debe registrar al menos una huella del operador, el cual debe estar registrado biométricamente en la Institución.
Análisis de parámetros de calidad	M	Conforme a NFIQ.
Limpieza	MP	Limpiar el plato antes de cada captura de huellas dactilares para lectores ópticos.

Iluminación	MP	Para dispositivos ópticos evitar fuentes de luz sobre el dispositivo de captura.
Recaptura	M	En caso de no obtener los parámetros de calidad mínimos, al menos 3 intentos por huella.
Transmisión		
Compresión imágenes de 500 puntos por pulgada (ppi, por su siglas en inglés)	M	Compresión única a partir de imagen RAW. WSQ máximo 10:1.

Decisión: M->Mandatorio O->Opcional MP->Mejor práctica

En caso de que las aplicaciones, procesos, parámetros o dispositivos utilizados en la captura de huellas dactilares, no se apeguen a los requisitos del presente anexo, las Instituciones deberán someterlos a la aprobación de la Comisión. No obstante lo anterior, tratándose de la captura de huellas dactilares de los clientes de las Instituciones, en ningún caso esta podrá ser menor a seis huellas, salvo por la excepción prevista en este anexo.

Excepción a la captura de huellas dactilares

En caso de que los clientes, empleados, directivos y funcionarios de las Instituciones estén imposibilitados de manera permanente para plasmar sus huellas dactilares en los respectivos lectores, se deberá precisar que no es posible realizar la captura de la imagen de las huellas dactilares por amputaciones, injertos, malformación, lesión permanente, prótesis, enfermedad, entre otras.

En todo caso, deberá capturarse el mayor número de huellas posibles, haciendo las anotaciones correspondientes en el expediente.

Autenticación utilizando la base de datos de huellas dactilares de las propias Instituciones

Para el proceso mediante el cual se haga la lectura de huellas dactilares para efectos de autenticación (cotejo 1 a 1) de clientes ya registrados, y su uso como Factor de Autenticación Categoría 4, en su caso, los requerimientos de captura de imagen son los siguientes:

Resolución del escáner (puntos por pulgada)	Profundidad (pixeles)	Rango dinámico mínimo (niveles de gris)
300	4 bits	12
500	8 bits	80

PARÁMETRO	DECISIÓN	OBSERVACIÓN
Autenticación		
Imagen Capturada		
Número de dedos	O	1 a 4 dependiendo el tipo de lector.
Cualquier dedo	O	Sí. La muestra contra todos los registros del usuario.
Recaptura	O	Sí. Se sugiere un mínimo de tres intentos.
Dispositivos		
Móvil	M	Certificados EFTS anexo F o PIV FAP 30.
Dual	M	Certificados EFTS anexo F FAP 45.
Decadactilares (4-4-2)	M	Certificados EFTS anexo F FAP 60.
Unidactilar	O	Se recomienda PIV.
Transmisión		
Formato	O	Alguno de los siguientes: Formato Propietario, Formato RAW, imagen comprimida con los estándares ANSI INCITS 378 o ISO/IEC 19794-2.

Decisión: M->Mandatorio O->Opcional MP->Mejor práctica

II. Lineamientos de operación para reconocimiento facial

En caso de que las Instituciones determinen obtener de sus clientes algún elemento de reconocimiento facial, las aplicaciones y dispositivos utilizados en el proceso de captura de elementos faciales, deberán considerar al menos los siguientes requerimientos:

PARÁMETRO	DECISIÓN	OBSERVACIÓN
Captura de imagen facial		
Imagen Capturada	M	2D Frontal completa, 24 bits a color distancia entre ojos mínimo 90 pixeles.
Requerimientos digitales y fotográficos	M	Estándar ISO 19794-5 sección 7.3,7.4, 8.3 y 8.4.
Postura	M	Debe permitir una rotación de al menos ±5° frontal en cualquier dirección (arriba, abajo, izquierda, derecha).
Expresión	M	Expresión neutral del rostro. Se deben evitar sonrisas, guiños, etc. Mirada al lente de la cámara (con excepción de impedimentos físicos).
Iluminación	M	Equilibrada y distribuida en cada parte del rostro. Para lograr tonos de piel natural y evitar ojos rojos.
Profundidad de Campo	M	La pose central del rostro completa estará en foco desde la coronilla hasta la barbilla y desde la nariz hasta las orejas.
Lentes	M	No se permitirá el uso de armazón de cualquier tipo.
Accesorios	M	Solo se permiten accesorios médicos (sin sombreros, ni accesorios que cubran el rostro).
Impedimentos para la toma	M	Ojos cerrados. Cabello cubriendo los ojos o la frente. Elementos que obstruyan la frente.
Vello Facial	M	Está permitido.
PARÁMETRO	**DECISIÓN**	**OBSERVACIÓN**
Fondo	O	Se empleará un fondo uniforme de color claro que contraste con el rostro y el cabello, se recomienda gris pálido o blanco.
Operación	M	Ambiente controlado de iluminación.
Asistido	M	Sí.
Segmentación y extracción de características	M	Recorte de acuerdo a estándar ICAO. Extracción de características automáticas por software.
Revisión de calidad	M	Automáticas por software se debe evaluar el estándar ICAO para la calidad de la imagen.
Autenticación		
Captura de Imagen	O	Igual que en captura de imagen facial.
Numero de Imágenes	O	Una frontal completa.

Decisión: M->Mandatorio O->Opcional MP->Mejor práctica

El proceso de captura de elementos para el reconocimiento facial debe impedir que un empleado, directivo o funcionario de la Institución registre sus propias características en sustitución de las del cliente. Para efectos de lo anterior, previo a que inicie la captura de la información de clientes, las Instituciones deberán asegurarse de que los datos de sus empleados, directivos y funcionarios hayan sido capturados previamente. Para lo anterior, las Instituciones deberán auxiliarse del o los responsables de las funciones de Contraloría Interna para que verifique lo previsto en este párrafo.

III. GLOSARIO

ANSI: *American National Standards Institute,* de los Estados Unidos de América.

Autenticación: El Proceso mediante el cual se verifica la identidad del Usuario con los datos biométricos de huellas dactilares o del rostro que las Instituciones hayan obtenido previamente. Este proceso implica búsquedas de patrones almacenados de un solo individuo (1 a 1).

Deduplicación: La técnica especializada de compresión de datos utilizada para evitar copias duplicadas de estos.

EFTS (por sus siglas en inglés *Electronic Fingerprint Transmission Specifications*): Las especificaciones para transmisión de información biométrica de la Oficina Federal de Investigación de los Estados Unidos de América (FBI).

FAP (por sus siglas en inglés *FingerPrint Acquisition Profile*): Es una subdivisión de las categorías aplicadas a los dispositivos para adquisición de huellas basada en dimensiones, número de dedos simultáneos a capturar, calidad de la imagen. Cuando se acompaña de un número (30, 45, 60) este indica el área de captura en pulgadas (45=1.6 x 1.5; 60=3.2 x 3.0, etc.).

ICAO: El estándar para fotografías en pasaportes emitido por la *International Civil Aviation Organisation.*

INCITS *(*por sus siglas en inglés *InterNational Committee for Information Technology Standards)*: El foro central de los Estados Unidos de América, dedicado a la creación de estándares para la innovación tecnológica.

ISO/IEC: El estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

NFIQ: *NIST Fingerprint Image Quality.* Los estándares de calidad de las imágenes de huellas dactilares definido por el NIST.

NIST: *National Institute of Standards and Technology.*

PIV: El estándar definido por el NIST para verificación de huellas dactilares 1-a-1 (comparación de una huella contra un registro).

Plato: La superficie de captura del dispositivo de captura de huellas dactilares.

RAW: El formato de captura de la imagen en crudo (sin procesar) de una huella dactilar.

Segmentación: El proceso mediante el cual se individualiza la imagen de la huella dactilar de cada dedo, con base en una imagen comprimida con WSQ o bien una sola imagen RAW obtenida del lector, para conseguir hasta cuatro imágenes independientes, una de cada dedo.

Slap Seg II Test: La prueba que evalúa la precisión con que el algoritmo segmenta imágenes en capturas multi-dedos.

WSQ (por sus siglas en Inglés *Wavelet Scalar Quantization*): El estándar creado por el FBI que define el formato para la compresión de imágenes de huellas dactilares.

ANEXO 72

Indicadores de seguridad de la información

El oficial en jefe de seguridad de la información de la Institución, en relación con los indicadores de seguridad de la información a que se refiere la fracción XII del Artículo 168 Bis 14, de las presentes disposiciones, deberá:

1. Evaluar dichos indicadores, los cuales deberán ajustarse a los umbrales contenidos en este anexo para cada indicador. En caso de definir umbrales diferentes, deberá documentar el motivo, el cual deberá estar alineado al nivel de tolerancia al riesgo de la Institución.

2. Definir planes de remediación para aquellos riesgos en los que los resultados de la evaluación arrojen valores que se encuentren dentro de los umbrales medios y altos de riesgo establecidos en el presente anexo o, en su caso, aquellos definidos por la Institución, siempre que estos se encuentren en un umbral alto por, al menos, dos periodos consecutivos.

3. Dar mantenimiento continuo, ya sea para agregar, eliminar o actualizar los indicadores claves de riesgo y de desempeño de seguridad de la información ya existentes, los cuales siempre deberán estar alineados a la estrategia de la Institución y al Plan Director de Seguridad de la información de esta.

4. Medir y evaluar su evolución con la periodicidad indicada en las siguientes tablas, o antes en caso de eventos inusuales.

5. En caso de que no apliquen todos los supuestos, indicar que no son aplicables y explicar el motivo.

El tipo, subtipo y sub clase de eventos en los que se encuentran clasificados cada uno de los indicadores que se enuncian a continuación, tienen su fundamento en la Sección II del Anexo 12-A de las presentes disposiciones:

Tipo	Definición	Sub Tipo	Sub Clase de Eventos	Ejemplos
I. Fraude Interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente, o bien, soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la Institución.	1.1 Actividades no autorizadas.	1.1.1 Operaciones no reveladas (intencionalmente). 1.1.2 Operaciones no autorizadas (con pérdidas pecuniarias). 1.1.3 Valoración errónea de posiciones (intencional).	Operaciones no comunicadas; operaciones no autorizadas (con pérdidas pecuniarias); valoración errónea de posiciones, y omisión intencional de normativa.
		1.2 Robo y Fraude Internos.	1.2.1 Fraude / fraude crediticio / depósitos sin valor. 1.2.2 Extorsión / malversación / robo. 1.2.3 Apropiación indebida de activos. 1.2.4 Destrucción dolosa de activos. 1.2.5 Falsificación Interna. 1.2.6 Utilización de cheques sin fondos. 1.2.7 Contrabando. 1.2.8 Apropiación de cuentas, de identidad, entre otros. 1.2.9 Incumplimiento / evasión de impuestos (intencional). 1.2.10 Cohecho. 1.2.11 Abuso de información privilegiada (no a favor de la empresa).	Robo; malversación; apropiación indebida; destrucción de activos; falsificaciones; suplantación de identidad; y cohechos; manipulación de cuentas.
		1.3. Seguridad de los sistemas.	1.3.1 Vulneración de sistemas de seguridad. 1.3.2 Daños por ataques informáticos. 1.3.3 Robo de información (con pérdidas pecuniarias). 1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.	Abuso y utilización de información privilegiada o confidencial; alteración de aplicaciones informáticas; robo de contraseñas, y accesos informáticos prohibidos.
II. Fraude Externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	2.1 Hurto y Fraude Externos.	2.1.1 Robo / estafa / extorsión /cohecho. 2.1.2 Falsificación Externa / Suplantación de personalidad. 2.1.3 Utilización fraudulenta de cheques. 2.1.4 Uso y/o divulgación de información privilegiada. 2.1.5 Espionaje industrial. 2.1.6 Contrabando.	Documentaciones falsificadas o manipuladas (cheques, transferencias, etc.); suplantación de identidad; disposiciones indebidas; monedas falsas; billetes deteriorados o fuera de curso legal; robos en las dependencias de la Institución, en las valijas internas, transportes de efectivo o en paquetes postales, y uso indebido de tarjetas robadas, falsificadas, robadas o en listas negras.
		2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad. 2.2.2 Daños por ataques informáticos. 2.2.3 Robo de información (con pérdidas pecuniarias). 2.2.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.	Acceso informático no autorizado; manipulación de aplicaciones informáticas; daños por ataques informáticos, y robo de información.
VI. Incidencias en el Negocio y Fallos en los Sistemas	Pérdidas derivadas de incidencias en el negocio y de fallas en los sistemas.	6.1 Sistemas	6.1.1Hardware. 6.1.2 Software. 6.1.3 Telecomunicaciones. 6.1.4 Interrupción / incidencias en el suministro.	Interrupción / incidencias en los suministros y líneas de comunicación; errores en los programas informáticos; fallos en hardware y software; sabotajes; interrupciones del negocio; fallos informáticos y programación de virus.

ID	Nombre	Descripción	Dominio	Tipo	Sub Tipo	Sub Clase de Eventos	Tipo de Indicador	Periodo	Unidad de Medi-ción	Cálculo	Variable X	Variable Y	Riesgo Alto	Riesgo Medio	Riesgo Bajo
KRI0001	Incidentes mediante ataques directos contra los sistemas internos.	Número de incidentes que hayan sido originados por ataques hacia los sistemas internos de la Institución, en el periodo establecido.	Ataques lógicos.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Reactivo.	Trimestral.	Cantidad.	Variable X	Número de casos de incidentes identificados.	-	Más de 1.	Igual a 1.	Igual a 0.
KRI0002	Casos de fraude en Banca Electrónica.	Porcentaje de casos donde se identifica un fraude, que haya sido originado por ataques hacia los sistemas de banca electrónica de la Institución, en el periodo establecido.	Ataques lógicos.	II. Fraude Externo	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Reactivo.	Mensual.	Porcentual.	(X/Y)*100	Número de casos de fraude en banca electrónica.	Número de usuarios de banca electrónica activos.	Más del .01 %.	Entre el 0.005 % y el 0.01 %.	Menos del 0.005 %.
KRI0003	Equipos de la Infraestructura Tecnológica de los que se gestiona su configuración de seguridad.	Porcentaje de equipos de Infraestructura Tecnológica dentro de la plataforma y/o proceso de revisión de estándares de configuración segura, con respecto al total de los equipos de la Institución durante el periodo establecido.	Cumplimiento.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Preventivo.	Mensual.	Porcentual.	(X/Y)*100	Número de equipos dentro de la plataforma o proceso de revisión de estándares de configuración segura.	Número total de equipos.	Menos del 85 %.	Entre 85 % y 95 %.	Más de 95 %.
KRI0004	Nivel de cumplimiento de configuración segura de servidores UNIX/Linux.	Porcentaje promedio de nivel de cumplimiento de servidores UNIX/Linux contemplados dentro de la herramienta y/o proceso de revisión de estándares de configuración segura.	Cumplimiento.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Preventivo.	Mensual.	Promedio porcentual.	Promedio(X)	% de cumplimiento del estándar de configuración segura de cada uno de los Servidores UNIX/Linux.	-	Menos del 90 %.	Entre 90 % y 95 %.	Más de 95 %.
KRI0005	Usuarios con roles y perfiles inadecuados.	Porcentaje de usuarios con perfiles inadecuados dentro de las aplicaciones de la Institución, con respecto al total de usuarios en todas las aplicaciones de la Institución.	Cumplimiento.	I. Fraude Interno	1.3. Seguridad de los sistemas.	1.3.3 Robo de información (con pérdidas pecuniarias). 1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.	Correctivo.	Semestral.	Porcentual.	(X/Y)*100	Número de usuarios con perfiles incorrectos, considerando todas las aplicaciones.	Número total de usuarios considerando todas las aplicaciones.	Más del 3 %.	Entre 1% y 3 %.	Menos del 1 %.
KRI0006	Aplicaciones sin roles y perfiles.	Porcentaje de aplicaciones las cuales no poseen la capacidad un perfilamiento de roles y permisos, o que dichos perfiles no están implementados, esto con respecto al total de aplicaciones.	Cumplimiento.	I. Fraude Interno.	1.3. Seguridad de los sistemas.	1.3.3 Robo de información (con pérdidas pecuniarias). 1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de aplicaciones sin capacidad de perfilamiento, o perfilamiento no implementado.	Número total de aplicaciones.	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %.

KRI0007	Incidentes de seguridad de la información en general	Número total de incidentes reportados durante el periodo establecido referentes a seguridad de la información.	Información.	Aplica a: I. Fraude Interno II. Fraude Externo VI. Incidencias en el Negocio y Fallos en los Sistemas.	Aplican a: 1.3. Seguridad de los sistemas 2.2 Seguridad de los Sistemas. 6.1 Sistemas.	Aplican a: 1.3.1 Vulneración de sistemas de seguridad 1.3.2 Daños por ataques informáticos. 1.3.3 Robo de información (con pérdidas pecuniarias). 1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización. 2.2.1 Vulneración de sistemas de seguridad. 2.2.2 Daños por ataques informáticos. 2.2.3 Robo de información (con pérdidas pecuniarias). 2.2.4 Utilización inadecuada de claves de acceso y/o niveles de autorización. 6.1.1Hardware. 6.1.2 Software. 6.1.3 Telecomunicaciones. 6.1.4 Interrupción / incidencias en el Suministro	Reactivo.	Mensual.	Cantidad.	Variable X.	Número de incidentes de seguridad. de la información	-	Más de 5.	De 2 a 5.	Menos de 2.
KRI0008	Plataformas tecnológicas obsoletas y/o desactualizadas	Porcentaje de plataformas tecnológicas que se encuentran sobre versiones obsoletas y/o sin soporte por el fabricante	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Semestral	Porcentual.	(X/Y)*10.	Número de plataformas tecnológicas obsoletas.	Total de plataformas tecnológicas.	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %
KRI0009	Caídas de sistemas relacionados con la red de cajeros automáticos.	Número de caídas de sistemas relacionados con la red de cajeros automáticos mayores a 10 minutos.	Infraestructura.	VI. Incidencias en el Negocio y Fallas en los Sistemas.	6.1 Sistemas.	6.1.4 Interrupción / incidencias en el Suministro.	Reactivo.	Mensual.	Cantidad.	Variable X.	Numero de caídas de sistemas.	-	Más de 1.	Igual a 1.	Igual a 0.
KRI0010	Incidentes de seguridad por vulnerabilidades de sistemas provistos por proveedores (terceros).	Porcentaje de incidentes de seguridad causados por vulnerabilidades en sistemas e infraestructura tecnológica provistos por proveedores (terceros) que no pertenezcan a la nómina de la institución, reportados durante el periodo establecido, con respecto al total de incidentes de seguridad.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad. 2.2.2 Daños por ataques informáticos. 2.2.3 Robo de información (con pérdidas pecuniarias). 2.2.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.	Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de incidentes de seguridad de atribuidos a vulnerabilidades en sistemas provistos por proveedores (terceros).	Número total de incidentes de seguridad.	Más del 5 %.	Entre 0.1 % y 5 %.	Menor a 0.1 %.

KRI0011	Vulnerabilidades críticas pendientes de corregir detectadas en las pruebas de hackeo ético.	Número de vulnerabilidades en los sistemas de información que, de acuerdo con las pruebas de hackeo ético, se cataloguen como críticas, las cuales tengan más de un mes de antigüedad a partir de su fecha de detección.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Preventivo.	Mensual.	Cantidad.	Variable X.	Número de vulnerabilidades críticas pendientes de corregir con antigüedad de más de un mes.	-	Más de 2.	Entre 1 y 2.	Igual a 0.
KRI0012	Indisponibilidad de los sistemas de TI.	Porcentaje promedio del tiempo de indisponibilidad de los sistemas contra el tiempo total del periodo establecido.	Infraestructura.	VI. Incidencias en el Negocio y Fallas en los Sistemas.	6.1 Sistemas.	6.1.4 Interrupción / incidencias en el Suministro.	Reactivo.	Mensual.	Promedio Porcentual.	Promedio(X).	Promedio de tiempo de indisponibilidad de los sistemas de TI.	-	Más del 0.5 %.	Entre 0.25 % y 0.5 %.	Menos de 0.25 %.
KRI0013	Indisponibilidad de banca electrónica.	Porcentaje del tiempo indisponibilidad contra el tiempo total del sistema de banca electrónica contra el mes en cuestión.	Infraestructura.	VI. Incidencias en el Negocio y Fallos en los Sistemas.	6.1 Sistemas.	6.1.4 Interrupción / incidencias en el Suministro.	Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Tiempo de indisponibilidad de la banca electrónica.	Tiempo total establecido para la banca electrónica.	Más del 0.25 %.	Entre 0.15 % y 0.25 %.	Menos de 0.15 %.
KRI0014	Incidentes críticos y de alta prioridad en ambientes productivos.	Porcentaje de incidentes calificados como críticos y de alta prioridad en ambientes de producción respecto al total de incidentes en producción.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de incidentes en producción calificados como críticos.	Número total de incidentes en producción.	Mayor o igual a 0.5 %.	Mayor a 0% y menor 0.5 %.	Igual a 0 %.
KRI0015	Componentes de la infraestructura tecnológica expuestos a internet sin pruebas de hackeo ético y/o análisis de vulnerabilidades.	Porcentaje de los componentes de la infraestructura tecnológica de la organización expuestos hacia internet a los cuales no se haya realizado hackeo ético o análisis de vulnerabilidades, con respecto al total de equipos en más de 3 meses.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de activos expuestos a internet que no hayan realizado pruebas de hackeo ético o análisis de vulnerabilidades.	Número de activos expuestos a internet.	Más del 3 %.	Entre el 1 % y 3 %.	Menos del 1 %.
KRI0016	Vulnerabilidades críticas pendientes de corregir detectadas en los análisis de vulnerabilidades.	Número de vulnerabilidades en los sistemas de información que, de acuerdo con los análisis de vulnerabilidades se cataloguen como críticas, las cuales, tengan más de un mes de antigüedad a partir de su fecha de detección.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Cantidad.	Variable X.	Número total de vulnerabilidades críticas.	-	Más de 2	Entre 1 y 2	Igual a 0

KRI0017	Casos de fraude reportados por los clientes de banca electrónica.	Porcentaje de casos de fraude reportados por los clientes de la banca electrónica de la Institución, considerando el número total de clientes de banca electrónica en el periodo establecido.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de casos de fraude reportados en banca electrónica.	Número de clientes de banca electrónica.	Más de 0.005 %	Entre 0.003 % y 0.005 %	Menor a 0.003 %
KRI0018	Infraestructura Tecnológica obsoleta y/o sin soporte.	Cantidad de equipos e Infraestructura Tecnológica, que se encuentran en versiones obsoletas o sin soporte, en comparación con toda la infraestructura de IT activa en el periodo establecido.	Infraestructura.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de equipos e infraestructura obsoleta.	Número total de equipos activos.	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %.
KRI0019	Servidores sin solución *antimalware.*	Porcentaje de servidores sin *antimalware* respecto del total de servidores.	*Malware.*	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores sin *antimalware*.	Número total de servidores.	Más del 6 %.	Entre 3% y 6 %.	Menor a 3 %.
KRI0020	Servidores con firmas de *antimalware* desactualizadas.	Porcentaje de servidores con firmas de *antimalware (malware signatures)* desactualizados respecto del total de servidores con *antimalware* en cada Institución	*Malware.*	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores con firmas *antimalware* desactualizadas.	Número total de servidores con *antimalware*.	Más del 6 %	Entre 3% y 6 %	Menor a 3 %
KRI0021	*Workstations* sin solución *antimalware*	Porcentaje de *workstations* sin *antimalware* con respecto al total de equipos	*Malware.*	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de *workstations sin antimalware.*	Número total de *workstations.*	Más del 8 %.	Entre 4% y 8 %.	Menor a 4 %.
KRI0022	*Workstations* con firmas de *antimalware* desactualizadas.	Porcentaje de las *workstations* que cuentan con las firmas de antimalware *(malware signatures)* desactualizadas con respecto al total de equipos de cómputo con antimalware instalado.	Malware.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de *workstations* con firmas *antimalware* desactualizadas.	Número de *workstations* con *antimalware.*	Más del 8 %.	Entre 4% y 8 %.	Menor a 4 %.
KRI0023	Incidentes de seguridad atribuidos a personal de proveedores (terceros).	Porcentaje de incidentes de seguridad relacionados a personal de proveedores (terceros) que no pertenezcan a la nómina de la Institución, reportadas durante el periodo establecido, con respecto al total de incidentes de seguridad.	Incidentes.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de incidentes de seguridad relacionados con personal de proveedores (terceros).	Número de incidentes de seguridad total de personal de proveedores (terceros).	Más del 5 %.	Mayor a 0 % y menor 5 %.	Igual a 0 %.
KRI0024	Servidores con versiones de sistema operativo obsoletas.	Porcentaje total de servidores con versiones de sistema operativo obsoletas comparado contra número total de servidores.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores con versiones de sistema operativo obsoletas.	Número total de servidores.	Más de 10 %.	Entre 5% y 10 %.	Menor a 5 %.

KRI0025	Aplicaciones en producción con cumplimiento parcial o deficiente de los controles de seguridad.	Porcentaje de las aplicaciones en producción con cumplimientos parciales o deficientes, con respecto a las políticas de seguridad establecidas, en cuestiones de seguridad, con respecto al total de aplicaciones.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de controles de seguridad deficientes en aplicaciones en producción.	Número total de controles de seguridad.	Más de 5 %.	Entre 2 % y 5 %.	Menos de 2 %.
KRI0026	*Data base managers (DBM)* con versiones de tecnología obsoletas o no soportadas.	Porcentaje de manejadores de *data base managers(DBM),* los cuales son versiones de tecnologías obsoletas o no soportadas por el fabricante, en comparación con el total de *data base managers (DBM)* activos en el periodo establecido.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de *data base managers (DBM)* obsoletas o no soportadas.	Número total *data base managers* (DBM).	Más del 10 %.	Entre 5 % y 10 %.	Menos del 5 %.
KRI0027	Aplicaciones obsoletas o no soportadas.	Porcentaje de aplicaciones dentro de la Institución, las cuales se encuentran obsoletas o sin soporte por el fabricante, con relación a todas las aplicaciones activas durante el periodo establecido.	Software.	II. Fraude Externo. VI. Incidencias en el Negocio y Fallos en los Sistemas.	2.2 Seguridad de los Sistemas. 6.1 Sistemas.	2.2.1 Vulneración de sistemas de seguridad. 6.1.2 Software.	Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de aplicaciones obsoletas o no soportadas.	Total de aplicaciones activas.	Más de 5 %.	Entre 2 % y 5 %.	Menos de 2 %.
KRI0028	Servidores Windows y UNIX/Linux sin cobertura de parches de seguridad.	Porcentaje de servidores sin los parches de seguridad más recientes en sistemas operativos Windows y UNIX/Linux, con respecto al total de servidores activos durante el periodo establecido.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores sin los parches de seguridad más recientes instalados.	Total de servidores.	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %.
KRI0029	*Workstations* sin cobertura de parches de seguridad.	Porcentaje de *workstations* sin los de parches de seguridad más recientes indistinto del sistema operativo de que se trate, con respecto al total de *workstations* de la institución.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Correctivo.	Mensual.	Porcentual.	(X/Y))*100.	Número *workstations* sin los parches de seguridad más recientes instaladas totales.	Número de *workstations* totales.	Más del 3 %.	Entre 1 % y 3 %.	Menos del 1 %.
KRI0030	*Data base managers (DBM)* sin cobertura de parches de seguridad.	Porcentaje de *data base managers (DBM)* sin cobertura de los parches de seguridad más recientes, con respecto al total de *data base managers (DBM)* durante el periodo establecido.	Software.	II. Fraude Externo.	2.2 Seguridad de los Sistemas.	2.2.1 Vulneración de sistemas de seguridad.	Preventivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de *data base managers (DBM)* sin cobertura de parches de seguridad.	Número total de *data base managers (DBM).*	Más del 5 %.	Entre 2 % y 5 %.	Menos del 2 %.

ACUERDO por el que se desincorpora del régimen de dominio público de la Federación y se autoriza su aportación a favor de la Secretaría de Turismo por conducto del Fondo Nacional de Fomento al Turismo (FONATUR), del inmueble federal con superficie de 277-79-64 hectáreas, denominado "Yeneka Lote 17, fracción I", ubicado en Zona Federal Carretera La Paz – San José del Cabo en el Municipio de Los Cabos, Estado de Baja California Sur, con Registro Federal Inmobiliario número 3-3491-5.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Hacienda y Crédito Público.- Instituto de Administración y Avalúos de Bienes Nacionales.- Dirección General de Administración del Patrimonio Inmobiliario Federal.

ACUERDO por el que se desincorpora del régimen de dominio público de la Federación y se autoriza su aportación a favor de la Secretaría de Turismo por conducto del Fondo Nacional de Fomento al Turismo (FONATUR), del inmueble federal con superficie de 277-79-64 hectáreas, denominado "Yeneka Lote 17, fracción I", ubicado en Zona Federal Carretera La Paz – San José del Cabo en el Municipio de Los Cabos, Estado de Baja California Sur, con Registro Federal Inmobiliario número 3-3491-5.

JULIO CÉSAR GUERRERO MARTÍN, Presidente del Instituto de Administración y Avalúos de Bienes Nacionales, Órgano Desconcentrado de la Secretaría de Hacienda y Crédito Público, con fundamento en lo dispuesto por los artículos 31 fracciones XXIX y XXX, de la Ley Orgánica de la Administración Pública Federal; 6 fracción XX, 11 fracción I, 29 fracciones I, II y VI, 84 fracción X, 92, 93, 95, 99 fracción II y 101 fracción VI, de la Ley General de Bienes Nacionales; 2o. apartado D fracción VI, 98-C, del Reglamento Interior de la Secretaría de Hacienda y Crédito Público y 1, 2 fracción X, 3 fracción X y 6 fracción XXXIII, del Reglamento del Instituto de Administración y Avalúos de Bienes Nacionales, adicionado mediante el Decreto por el que se reforman y adicionan diversas disposiciones del Reglamento Interior de la Secretaría de Hacienda y Crédito Público y del Reglamento del Instituto de Administración y Avalúos de Bienes Nacionales, publicado en el Diario Oficial de la Federación el 12 de enero de 2017; y

CONSIDERANDO

PRIMERO. - Que dentro de los bienes sujetos al régimen de dominio público de la Federación, se encuentra el inmueble con superficie de 277-79-64 hectáreas, denominado "Yeneka Lote 17, fracción I", ubicado en Zona Federal Carretera La Paz – San José del Cabo en el Municipio de Los Cabos, Estado de Baja California Sur, con Registro Federal Inmobiliario número 3-3491-5.

SEGUNDO. - Que el inmueble a que se refiere el Considerando precedente, pertenece a un inmueble de mayor extensión con superficie total de 939,489-00-00 hectáreas, y se acredita mediante Declaratoria de propiedad nacional del terreno denominado Zona Sur del Paralelo 24°00, Municipio de La Paz y Los Cabos en Baja California Sur, publicada en el Diario Oficial de la Federación el 31 de julio de 1987, inscrita en el Registro Público de la Propiedad Federal, bajo el Folio Real número 147692 de 01 de diciembre de 2016.

TERCERO. – Que las medidas y colindancias del inmueble materia del presente se consignan en el plano registrado y aprobado con número DRPCI/6349/3-3491-5/2018/T, del 20 de noviembre de 2018, por la Dirección del Registro Público y Control Inmobiliario de la Dirección General de Política y Gestión Inmobiliaria, unidad administrativa del Instituto de Administración y Avalúos de Bienes Nacionales, órgano desconcentrado de la Secretaría de la Hacienda y Crédito Público;

CUARTO. – Que la Secretaría de Desarrollo Agrario, Territorial y Urbano, mediante Acuerdo de fecha 06 de abril de 2018, publicado en el Diario Oficial de la Federación de 26 de abril de 2018, puso a disposición de la Secretaría de Hacienda y Crédito Público a través del Instituto de Administración y Avalúos de Bienes Nacionales, el inmueble que nos ocupa para que fuera destinado al patrimonio de la Secretaría de Turismo, por conducto del Fondo Nacional de Fomento al Turismo. Que se publicó en el Diario Oficial de la Federación el 17 de julio de 2018, Nota Aclaratoria de la publicación en el Diario Oficial de la Federación del Acuerdo del seis de abril de dos mil dieciocho, la cual se realizó el día veintiséis de abril de dos mil dieciocho, por medio del cual la Secretaria de Desarrollo Agrario, Territorial y Urbano, pone a disposición de la Secretaria de Hacienda y Crédito Público, a través de la Dirección General del Patrimonio Inmobiliario Federal, dependiente del Instituto de Administración y Avalúos de Bienes Nacionales (INDAABIN), el predio denominado "YENEKA Lote 17 Fracción I", ubicado en el municipio de Los Cabos, en el estado de Baja California Sur, con una superficie de 277-79-64 hectáreas; a efecto de que en términos del artículo 57 de la Ley General de Bienes Nacionales, proceda a desincorporarlo a favor de Secretaria de Turismo, a través del Fondo Nacional de Fomento al Turismo (FONATUR).

QUINTO. - Que el Fondo Nacional de Fomento al Turismo, mediante oficio número DAF/AGS/246/2018 de 10 de agosto de 2018, solicitó formalmente al Instituto de Administración y Avalúos de Bienes Nacionales la aportación a su patrimonio del inmueble a que se refiere el Considerando Primero del presente Acuerdo, en el que se pretenden ejecutar la demanda de servicios, equipamiento y desarrollo habitacional que requiere el destino turístico de Los Cabos.

SEXTO.- Que el Comité de Aprovechamiento Inmobiliario de este Instituto de Administración y Avalúos de Bienes Nacionales, en su (4ª/18) Cuarta Sesión Extraordinaria del año 2018 celebrada el 20 de septiembre de 2018, emitió Acuerdo número (92/18 CAI) mediante el cual los miembros del Comité de Aprovechamiento Inmobiliario, acordaron por unanimidad de votos la opinión positiva para la emisión del Dictamen para Actos de Administración y Disposición, así como la desincorporación y aportación a la Secretaria de Turismo por conducto del Fondo Nacional de Fomento al Turismo;

SÉPTIMO. - Que la Dirección General de Política y Gestión Inmobiliaria, dependiente de este Instituto de Administración y Avalúos de Bienes Nacionales, el 31 de octubre del 2018, emitió Dictamen de no utilidad para un uso diverso del servicio público número DAAD/2018/051, respecto del inmueble materia de este Acuerdo;

OCTAVO. - Que la Dirección General de Administración del Patrimonio Inmobiliario Federal de este Instituto de Administración y Avalúos de Bienes Nacionales, de conformidad con lo previsto por el artículo 11, fracción V, del Reglamento de este Instituto, conoció y revisó desde el punto de vista técnico jurídico, la operación que se autoriza, asimismo, la documentación legal y técnica que sustenta la situación jurídica y administrativa del inmueble, y este Acuerdo obra en el expedientillo de trámite integrado por dicha Dirección General y fue debidamente integrada y cotejada con la que obra en el Sistema de Información Inmobiliario Federal y Paraestatal;

NOVENO. - Que con base en las consideraciones referidas y siendo propósito del Ejecutivo Federal dar al patrimonio inmobiliario federal el óptimo aprovechamiento, he tenido a bien expedir el siguiente:

ACUERDO

PRIMERO. - Se desincorpora del régimen de dominio público de la Federación el inmueble descrito en el Considerando Primero de este Acuerdo y se autoriza su aportación al Fondo de Nacional de Fomento al Turismo, para atender la creciente demanda de servicio, equipamiento y desarrollo habitacional que requiere el destino turístico de los Cabos, que contribuirá a la consolidación de ese polo turístico con su consecuente desarrollo económico, regional y nacional.

SEGUNDO. - El Instituto de Administración y Avalúos de Bienes Nacionales, ejercerá a nombre y representación de la Federación, los actos correspondientes para llevar a cabo la operación que se autoriza.

TERCERO. - Si el Fondo de Nacional de Fomento al Turismo, no utilizare el inmueble cuya aportación a su favor se autoriza o le diere un uso distinto al establecido en este Acuerdo sin la previa autorización del Instituto de Administración y Avalúos de Bienes Nacionales, o bien lo dejare de necesitar, dicho inmueble con todas sus mejoras y accesiones revertirá al patrimonio de la Federación. Esta prevención deberá insertarse en el título de propiedad que al efecto se expida.

CUARTO. – El Fondo Nacional de Fomento al Turismo, deberá nombrar en un plazo no mayor a 30 días posteriores a la publicación de este Acuerdo, a un funcionario, con nivel por lo menos de Director General o su equivalente, a fin de dar cumplimiento a las obligaciones previstas en la Ley General de Bienes Nacionales.

QUINTO.– El Instituto de Administración y Avalúos de Bienes Nacionales efectuara la entrega recepción del inmueble que en este acto se aporta al Fondo Nacional de Fomento al Turismo, dentro de los 30 días posteriores a la publicación del presente Acuerdo en el Diario Oficial de la Federación.

SEXTO. - Los impuestos, derechos, honorarios y gastos que se originen con motivo de la operación que se autoriza, serán cubiertos por el Fondo de Nacional de Fomento al Turismo, conforme a lo establecido en las disposiciones legales respectivas.

SEPTIMO. - El Instituto de Administración y Avalúos de Bienes Nacionales en el ámbito de sus atribuciones por conducto de la Dirección General de Administración del Patrimonio Inmobiliario Federal, vigilará el estricto cumplimiento de este Acuerdo.

OCTAVO.– Si dentro del término de un año contado a partir de la fecha de entrada en vigor de este Acuerdo no se hubiere celebrado el contrato correspondiente a la operación que se autoriza por causas imputables al Fondo de Nacional de Fomento al Turismo, determinadas por el Instituto de Administración y Avalúos de Bienes Nacionales, este Acuerdo quedará sin efectos, debiendo este Instituto publicar en el Diario Oficial de la Federación, un aviso en el que se dé a conocer esta circunstancia.

Este Acuerdo entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Sufragio Efectivo. No Reelección.

Ciudad de México, a 21 de noviembre de dos mil dieciocho.- El Presidente del Instituto de Administración y Avalúos de Bienes Nacionales, **Julio César Guerrero Martín**.- Rúbrica.

LISTA de valores mínimos para desechos de bienes muebles que generen las dependencias y entidades de la Administración Pública Federal.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Hacienda y Crédito Público.- Instituto de Administración y Avalúos de Bienes Nacionales.

LISTA DE VALORES MÍNIMOS PARA DESECHOS DE BIENES MUEBLES QUE GENEREN LAS DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA FEDERAL.

Con fundamento en los artículos 132 quinto párrafo de la Ley General de Bienes Nacionales; 31 fracción XXXIV de la Ley Orgánica de la Administración Pública Federal; 2 apartado D fracción VI y 98C del Reglamento Interior de la Secretaría de Hacienda y Crédito Público; 1, 3 fracciones VII, y XXIX, 4 fracción I, inciso a), 6 fracción XXXVI del Reglamento del Instituto de Administración y Avalúos de Bienes Nacionales; y en la norma segunda fracción XVIII de las Normas Generales para el registro, afectación, disposición final y baja de bienes muebles de la Administración Pública Federal Centralizada, el Instituto de Administración y Avalúos de Bienes Nacionales expide la siguiente:

LISTA DE VALORES MÍNIMOS PARA DESECHOS DE BIENES MUEBLES QUE GENEREN LAS DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA FEDERAL

C O N C E P T O	UNIDAD DE MEDIDA	VALOR UNITARIO PESOS
Aceite quemado	Litro	0.8820
Acero cobrizado (copperweld)	Kilogramo	1.3451
Acero inoxidable (baleros, instrumental médico dañado y pedacería)	Kilogramo	8.7731
Acero inoxidable 430	Kilogramo	8.7731
Acumuladores	Kilogramo	3.9401
Aisladores de porcelana	Kilogramo	0.4372
Alambre de cobre con papel	Kilogramo	61.9373
Alfombra y bajo alfombra	Kilogramo	0.8900
Aluminio	Kilogramo	9.5000
Aluminio granular	Kilogramo	19.4107
Artículos de porcelana con herraje	Kilogramo	0.5558
Aserrín	Kilogramo	0.0199
Balastra	Kilogramo	1.5102
Block de grafito	Kilogramo	13.6432
Boleto de metro	Kilogramo	0.6265
Bolsas de polietileno	Kilogramo	2.7696
Bronce	Kilogramo	114.2115
Cable aluminio (AAC)	Kilogramo	14.8921
Cable aluminio (ACSR)	Kilogramo	10.8803

Cable aluminio con forro	Kilogramo	11.4745
Cable armado (TAFP)	Kilogramo	21.7454
Cable cobre concéntrico	Kilogramo	48.3373
Cable cobre conductor (EKC y EKI)	Kilogramo	132.5757
Cable cobre y forro de plástico autosoportado	Kilogramo	29.6057
Cable cobre con forro de plomo (TA y TAP)	Kilogramo	15.6221
Cable cobre paralelo con forro	Kilogramo	28.1090
Cable de fuerza	Kilogramo	31.6566
Cable polilam	Kilogramo	39.5215
Cámara de hule	Kilogramo	0.4977
Carretes de madera:		
0.60 m.	Pieza	14.3484
0.80 m.	Pieza	29.1989
1.00 m.	Pieza	42.7972
1.20 m.	Pieza	64.5593
1.40 m.	Pieza	105.7597
1.60 m.	Pieza	115.0553
1.70 m.	Pieza	134.0622
1.80 m.	Pieza	143.7394
2.00 m.	Pieza	199.8534
2.20 m.	Pieza	289.7084
Cartón	Kilogramo	0.3820
Cartón de tapas	Kilogramo	0.5966
Cartoncillo (cubierta defectuosa)	Kilogramo	0.4040
Cartuchos de cinta para máquina de escribir	Kilogramo	2.3673
Catalizador IMP-TPC-1 usado y/o agotado	Kilogramo	0.0652
Cintas correctores IBM	Kilogramo	0.6540
Cobre desnudo	Kilogramo	98.7439
Conductores eléctricos de cobre con forro de plástico de diversos tipos y calibres	Kilogramo	38.0702
Corbatas de hule	Kilogramo	0.0815

Costales:		
a) Henequén y palma (cortados)	Pieza	0.2232
b) Yute capacidad de 40-50 Kgs.	Pieza	1.7184
c) Yute capacidad de 70-75 Kgs. (cortados transversalmente)	Pieza	0.3346
Cubeta para cera (plástico)	Pieza	3.2189
Cuchillas corta circuito con aislante de porcelana	Kilogramo	1.5130
Cuñetes:		
a) Capacidad de 50 Kgs.	Pieza	12.2426
b) Capacidad de 100 Kgs.	Pieza	19.3298
Desecho ferroso:		
a) Primera especial.- Acero al carbón, fierro dulce, accesorios de vía, sobrantes de piezas troqueladas, etc., que no requiere preparación (corte) para fundición.	Kilogramo	2.5420
b) Primera.- Acero al carbón, fierro dulce, cigüeñal de locomotora, durmiente metálico, bastidor de truck, placa proveniente de carros, tanques y toneles de ferrocarril, etc., que requiere preparación (corte) para fundición.	Kilogramo	1.7274
c) Segunda.- Alambre y cable de acero, fierro galvanizado, postes metálicos, tubería de acero, desecho mixto de fierro y lámina.	Kilogramo	1.1984
d) Tercera.- Fleje, lámina y cable galvanizado.	Kilogramo	1.0677
e) Mixto contaminado	Kilogramo	0.4202
Desecho ferroso proveniente de:		
a) Compactadoras	Kilogramo	4.0043
b) Motoconformadoras	Kilogramo	3.9462
c) Pavimentadoras	Kilogramo	3.5003
d) Petrolizadoras	Kilogramo	3.1639
e) Tractores	Kilogramo	3.8363
f) Tractores agrícolas	Kilogramo	3.6877
Desecho ferroso vehicular	Kilogramo	3.3521
Desperdicios alimenticios:		
a) Proveniente de cocina	Kg./lt.	0.2982
b) Proveniente de comedor y dietología	Kg./lt.	0.2615

c) Proveniente de planta	Kilogramo	0.2386
Durmientes de madera de 4a.	Pieza	4.8750
Ejes de carro de ferrocarril y locomotora	Kilogramo	3.1155
Escoria de bronce	Kilogramo	93.0073
Escoria de hierro	Kilogramo	0.4082
Esferas para máquina de escribir	Kilogramo	8.3720
Fierro colado	Kilogramo	1.4734
Garrafón:		**-**
a) Plástico de un galón	Pieza	0.3136
b) Plástico de 18 lts.	Pieza	1.5672
c) Plástico de 20 lts.	Pieza	1.7750
d) Plástico de 50 lts.	Pieza	4.3362
e) Vidrio de 20 lts.	Pieza	4.7200
Grasa de coco	Kilogramo	2.7403
Grasa de soya	Kilogramo	2.5842
Grasas diferentes especificaciones (contaminada)	Kilogramo	4.1881
Ladrillo refractario (pedacería)	Kilogramo	0.2190
Lata alcoholera	Pieza	4.4760
Latón	Kilogramo	92.0917
Leña común	Kilogramo	0.0428
Líquido fijador cansado con recuperación de gramos-plata por litro:		
a) Hasta 3.9 grs./lt.	Litro	14.0092
b) De 4.0 grs./lt. hasta 4.9 grs./lt.	Litro	18.0119
c) De 5.0 grs./lt. hasta 5.9 grs./lt.	Litro	22.0145
d) A partir de 6.0 grs./lt.	Litro	24.0159
Literas (tubulares)	Kilogramo	1.1984
Luminaria (desecho)	Kilogramo	1.3098
Llantas:		
a) Completas y/o renovables	Kilogramo	0.9775
b) Segmentadas y/o no renovables	Kilogramo	0.2038
Machimbradoras manuales	Kilogramo	8.1770

Madera creosotada	Kilogramo	0.0855
Madera de empaque	Kilogramo	0.2669
Madera proveniente del desmantelamiento de coches y carros de ferrocarril	Kilogramo	0.3525
Madera proveniente de tarimas	Kilogramo	0.7259
Mancuerna de carro y coche de ferrocarril	Kilogramo	2.7190
Medidores de energía eléctrica, de gas, registradores de potencia y factor de potencia	Kilogramo	1.2778
Papel archivo	Kilogramo	0.4238
Papel archivo con calca	Kilogramo	0.1591
Papel cesto	Kilogramo	0.0405
Papel con tubo	Kilogramo	0.8137
Papel de capa o lomo	Kilogramo	0.9175
Papel de revoltura	Kilogramo	0.2745
Papel kraft	Kilogramo	0.3209
Papel listado de computadora (forma continua)	Kilogramo	1.0806
Papel periódico	Kilogramo	0.4374
Papel pliego impreso	Kilogramo	0.4788
Papel proveniente de imprenta (impreso y recorte de bond ahuesado y cartulina)	Kilogramo	0.8190
Papel proveniente de revistas, publicaciones y folletos	Kilogramo	0.4083
Papel viruta color	Kilogramo	0.3747
Papel viruta de 2a. con goma	Kilogramo	0.3002
Piedra de esmeril	Kilogramo	0.1043
Pintura caduca y gelada	Litro	1.4401
Plástico	Kilogramo	1.1185
Plástico acrílico	Kilogramo	1.7240
Plomo	Kilogramo	31.2739
Plomo con clavo y pabilo	Kilogramo	26.9005
Polietileno	Kilogramo	1.1966

Polipropileno	Kilogramo	2.2208
Polvo de grafito	Kilogramo	0.3116
Postes de concreto	Pieza	32.8103
Postes de madera	Kilogramo	0.2480
Radiadores de ferrocarril y automotrices	Kilogramo	29.7015
Rebaba de acero tipo listón y granel	Kilogramo	0.4082
Rebaba de aluminio	Kilogramo	18.4417
Rebaba de bronce	Kilogramo	73.6971
Rebaba de cobre	Kilogramo	83.6897
Rebaba de fierro colado	Kilogramo	0.5479
Residuos de catalizador	Kilogramo	0.0516
Riel de ferrocarril:		
a) 4 Rayas mayor de 3.05 m. (sin cortar)	Kilogramo	2.6908
b) 4 Rayas menor de 3.05 m. (sin cortar)	Kilogramo	2.6309
Rodillos de computadora	Kilogramo	0.8251
Rueda de acero de carro y coche de ferrocarril	Kilogramo	2.9270
Sacos:		
a) Manta	Pieza	1.9250
b) Papel kraft y polietileno (multicapas)	Pieza	2.3306
c) Polipropileno	Pieza	3.3448
d) Polipropileno (pedacería)	Kilogramo	2.0108
Tambos de lámina capacidad de 200 lts.:		
a) Buenos	Pieza	54.0484
b) Regulares	Pieza	27.9265
c) Mal estado (picado o corroído)	Pieza	10.8625
Tambos de plástico capacidad de 200 lts.	Pieza	82.9000
Tarjeta IBM	Kilogramo	2.2214

Tela (recorte de maquila)	Kilogramo	0.9000
Tierra de plomo	Kilogramo	14.5689
Tierra de zinc	Kilogramo	17.3330
Transformadores de corriente	Kilogramo	4.8890
Transformadores de distribución y potencia con aceite	Kilogramo	3.0411
Transformadores de distribución y potencia sin aceite	Kilogramo	6.6106
Trapos:		
a) Colchas, cobijas, sábanas, cortinas, vestuarios, campos, portacharolas y otros de tela proveniente de los hospitales (limpios)	Kilogramo	7.5000
b) Desperdicios sucios y manchados (no contaminados)	Kilogramo	3.8500
Tubería admiralty	Kilogramo	80.8522
Tubería de cuproníquel	Kilogramo	180.8475
Tubería HK 40	Kilogramo	22.8236
Tubos de acero al carbón en tramos mayores de 3 m. de longitud con diámetro exterior:		
a) Hasta 33.40 mm. (1 5/16")	Kilogramo	27.0814
b) Mayor de 33.40 mm. hasta 114.30 mm. (4 1/2")	Kilogramo	19.8647
c) Mayor de 114.30 mm. hasta 219.08 mm. (8 5/8")	Kilogramo	15.1695
d) Mayor de 219.08 mm. hasta 406.40 mm. (16")	Kilogramo	12.3180
e) Mayor de 406.40 mm. hasta 1,219.20 mm. (48")	Kilogramo	9.6406
Tubos fluorescentes (rotos)	Kilogramo	0.0902
Vidrio pedacería	Kilogramo	0.0600
Zinc metálico (desecho)	Kilogramo	41.6686

Los valores de la presente lista no incluyen el Impuesto al Valor Agregado y entrarán en vigor al día siguiente de su publicación. Esta Lista estará vigente hasta en tanto no se emita una nueva Lista.

Sufragio Efectivo No Reelección.

Ciudad de México a 1 de noviembre de 2018.- El Presidente del Instituto de Administración y Avalúos de Bienes Nacionales, **Julio César Guerrero Martín**.- Rúbrica.

NOTIFICACIÓN mediante la cual se da a conocer el inicio del procedimiento administrativo para emitir la Declaratoria de Sujeción al Régimen de Dominio Público de la Federación, respecto del inmueble Federal que se señala, por encontrarse en el supuesto de lo establecido en el artículo 29 fracción IV en relación con el artículo 6 fracción VI, ambos de la Ley General de Bienes Nacionales.

NOTIFICACIÓN mediante la cual se da a conocer el inicio del procedimiento administrativo para emitir la Declaratoria de Sujeción al Régimen de Dominio Público de la Federación, respecto del inmueble Federal que se señala, por encontrarse en el supuesto de lo establecido en el artículo 29 fracción IV en relación con el artículo 6 fracción VI, ambos de la Ley General de Bienes Nacionales.

A LOS PROPIETARIOS Y/O POSEEDORES DE LOS PREDIOS COLINDANTES CON EL INMUEBLE FEDERAL QUE SE SEÑALA.

P R E S E N T E S

Con fundamento en lo dispuesto por el artículo 27 de la Constitución Política de los Estados Unidos Mexicanos; artículos 2, 17, 26, 31 fracciones XXIX, XXX y XXXIII de la Ley Orgánica de la Administración Pública Federal; 2, fracciones VI y VII, 3 fracción III, 4, 6 fracción VI, 10, 13, 28, fracciones I, III y VII, 29, fracción IV, 32 y 40 de la Ley General de Bienes Nacionales; 2o. apartado D fracción VI, 6 fracción XXXV y 98-C del Reglamento Interior de la Secretaría de Hacienda y Crédito Público, así como los artículos 1, 3 fracción X, 6 fracción XXXIII y 11 fracciones I y V del Reglamento del Instituto de Administración y Avalúos de Bienes Nacionales, ambos Reglamentos adicionados mediante Decreto por el que se reforman y adicionan diversas disposiciones del Reglamento Interior de la Secretaría de Hacienda y Crédito Público y del Reglamento del Instituto de Administración y Avalúos de Bienes Nacionales, publicado en el Diario Oficial de la Federación el 12 de enero de 2017; ARTÍCULO PRIMERO del Acuerdo delegatorio, emitido por la Presidente del Instituto de Administración y Avalúos de Bienes Nacionales, publicado en el Diario Oficial de la Federación el día 8 de marzo del 2017; 2, 3 fracción VI, 4, 8 y 10 de la Ley del Diario Oficial de la Federación y Gacetas Gubernamentales; 4 de la Ley Federal de Procedimiento Administrativo.

El Instituto de Administración y Avalúos de Bienes Nacionales, es un Órgano Desconcentrado de la Secretaría de Hacienda y Crédito Público, como lo disponen los artículos 2o. apartado D fracción VI, 6 fracción XXXV y 98-C del Reglamento Interior de esta última y 1 de su propio Reglamento, al cual le corresponde llevar el inventario, registro y catastro de los inmuebles federales, así como la administración, vigilancia, control, protección, adquisición, enajenación y afectación de inmuebles federales competencia de la propia Secretaría, de conformidad con los artículos 1, 3 fracción X y 11 fracciones I y V del Reglamento del Instituto de Administración y Avalúos de Bienes Nacionales, facultades que son ejercidas a través de la Dirección General de Administración del Patrimonio Inmobiliario Federal.

N O T I F I C A

El inicio del procedimiento para la emisión de la Declaratoria de Sujeción al Régimen de Dominio Público de la Federación, respecto del inmueble Federal, con el Registro Federal Inmobiliario, denominación, ubicación, superficie, medidas y colindancias correspondientes, señalados en el cuadro siguiente:

No.	RFI	Denominación ubicación y superficie	Orientación	Colindancia	Medidas Metros
1	9-17641-7	**"Policía Judicial Federal"** ubicado en Calle Jaime Nunó, N° 25, Colonia Morelos, C.P. 6200, Alcaldía Cuauhtémoc, Ciudad de México. Superficie de 694.00 metros cuadrados.	NORTE	Calle Jaime Nunó	16.75
			SUR	Lote 45	23.78
			OESTE	Propiedad Particular Casa 27 de Calle Jaime Nunó	31.00
			NOROESTE	Línea curva con Pancoupe Intersección de las Calles Jaime Nunó y la Cerrada de Libertad	11.75
			PONIENTE	Calle Cerrada de Libertad	21.42

Que en virtud de que el inmueble de mérito se encuentra bajo la posesión, control y administración de la Secretaría de Hacienda y Crédito Público a través de su Órgano Desconcentrado denominado Instituto de Administración y Avalúos de Bienes Nacionales, y con fundamento en el Art. 4 de la Ley Federal de Procedimiento Administrativo, **SE CONCEDE** un **PLAZO** de **CINCO DÍAS HÁBILES,** contados a partir del día siguiente de su publicación en el Diario Oficial de la Federación, para que por sí mismos o por medio de sus representantes legales, manifiesten su inconformidad mediante escrito libre dirigido a la Dirección General de Administración del Patrimonio Inmobiliario Federal, mismo que deberán acompañar de la documentación en la que se funde su dicho, presentándola en el domicilio ubicado en Avenida México número 151, Colonia Del Carmen, Código Postal 04100, Alcaldía Coyoacán, Ciudad de México.

En la Ciudad de México a los 14 días del mes de noviembre de dos mil dieciocho.- El Director General de Administración del Patrimonio Inmobiliario Federal, **Alan Daniel Cruz Porchini**.- Rúbrica.