CIRCULAR EXTERNA No.

PARA: **REPRESENTANTES LEGALES, MIEMBROS DEL CONSEJO DE ADMINISTRACIÓN O JUNTAS DIRECTIVAS, MIEMBROS JUNTA DE VIGILANCIA O COMITÉ DE CONTROL SOCIAL, REVISORES FISCALES Y ASOCIADOS DE ORGANIZACIONES DE LA ECONOMÍA SOLIDARIA**

DE: **LILIANA ANDREA FORERO GOMEZ – SUPERINTENDENTE (e)**

ASUNTO: **Por la cual se adiciona el Capítulo XVII al Título IV de la Circular Externa No. 20 de 2020, Circular Básica Jurídica**

FECHA: **Bogotá D.C.,**

Dentro de las facultades de la Superintendencia previstas en el artículo 36 de la Ley 454 de 1998, se encuentran entre otras, la señalada en el numeral 22 que prevé: *"Instruir a las instituciones vigiladas sobre la manera como deben cumplirse las disposiciones que rigen su actividad, fijar los criterios técnicos y jurídicos que faciliten el cumplimiento de tales normas y señalar los procedimientos para su cabal aplicación."*

Teniendo en cuenta que el auge de la digitalización de los servicios financieros, la mayor interconectividad de los agentes y la masificación en el uso de canales electrónicos, entre otros elementos, han derivado un incremento de la exposición a riesgos de seguridad de la información y cibernéticos, esta Superintendencia en ejercicio de sus facultades, y en aras de fortalecer la gestión relativa a este riesgo en las entidades vigiladas, imparte las siguientes instrucciones en complemento de aquellas relacionadas con la administración del riesgo operativo, para que de manera preventiva las organizaciones solidarias adopten mecanismos que minimicen su impacto, como un elemento que fortalezca la confianza de las entidades que conforman el sector solidario actual.

Por lo anterior, en ejercicio de las facultades otorgadas a esta Superintendencia en el numeral 22 del artículo 36 de la Ley 454 de 1998, y con miras a coadyuvar en el proceso de trasformación digital de las entidades sometidas a inspección, control y vigilancia, así como armonizar las disposiciones vigentes con los estándares internacionales en materia de seguridad de la información; se imparten las siguientes instrucciones:

PRIMERA: Adicionar el Capítulo XVII al Título IV de la de la Circular Básica Jurídica: *"Instrucciones sobre seguridad y calidad de la información para la prestación de los servicios financieros en las organizaciones vigiladas"*

SEGUNDA: La presente Circular entra a regir seis meses después del momento de su publicación.

TERCERA: Conforme con lo previsto en el inciso primero del artículo 65 de la Ley 1437 de 2011, la presente Circular rige a partir de la fecha de su publicación en el Diario Oficial.

De acuerdo con las anteriores instrucciones, se anexa el Capítulo XVII del Título IV de la Circular Básica Jurídica, objeto de inclusión.

Cordialmente,

LILIANA ANDREA FORERO GÓMEZ
Superintendente (e)

Anexo: Capítulo XVII del Título IV de la Circular Básica Jurídica

TÍTULO IV

CAPITULO XVII

INSTRUCCIONES SOBRE SEGURIDAD Y CALIDAD DE LA INFORMACIÓN PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS EN LAS ORGANIZACIONES VIGILADAS

INDICE

1.CONSIDERACIONES GENERALES 3
2.AMBITO DE APLICACIÓN 3
3.DEFINICIONES 3
4.ELEMENTOS CLAVE DEL DE LA INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION 4
4.1.Gobierno de seguridad de la información 4
4.1.1.Estrategia de Seguridad 4
4.1.2.Roles y responsabilidades 5
4.1.2.1.Consejo de Administración 5
4.1.2.2.Representante Legal 5
4.1.2.3.Auditoría interna o quien ejerza control interno 6
4.1.3.Estándar base para adaptar el Sistema de Seguridad de la Información 6
4.2.Riesgos de seguridad de la información 6
4.3.Sistema de Seguridad de la información 6
4.3.1.Descripción 7
4.3.2.Revisión 7
4.3.3.Aprobación 7
4.3.4.Publicación 7
4.3.5.Evaluación 7
4.3.6.Actualización 7
4.4.Recursos 7
4.4.1.Presupuesto 8
4.4.2.Competencia 8
4.4.3.Comunicación 8
4.5.Información documentada 8
4.5.1.Principios de seguridad de la información 8
4.5.2.Otra información documentada 8
4.5.3.Creación y actualización de la información documentada 9
4.5.4.Control de la información documentada 9
5.ETAPAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACION 9
5.1.Roles y Responsabilidades 9
5.2.Recursos humanos 9

6.REQUERIMIENTOS DE MEDIOS TECNOLÓGICOS Y SEGURIDAD DE LA INFORMACIÓN 0
6.1.Controles criptográficos 10
6.2.Protección contra códigos móviles o maliciosos 11
6.3.Intercambio de información 11
6.4.Respaldo de la información 12
6.5.Sincronización de Relojes 12
6.6.Controles de Acceso 12
6.7.Tele-Trabajo 13
6.8.Acceso a las redes WIFI 13
6.9.Aspectos no permitidos 13
6.10.Prestación de servicios por terceras partes 14
6.11.Gestión de Incidentes de Seguridad 14
6.12.Divulgación de Información 15
6.13.Inventario de activos 16
6.14.Cajeros Automáticos (ATM) 16
6.15.POS (incluye PIN Pad) 16
6.16.Centro de Atención Telefónica (Call Center, Contact Center) 17
6.17.Transacciones por Internet 17
6.18.Análisis de Vulnerabilidades 18
6.19.Seguridad física y del entorno. 18
6.20.Instalaciones y suministros 18
6.21.Planificación e implementación de la continuidad de la seguridad de la información 19
6.22.Reutilización o eliminación segura de equipos 20

TÍTULO IV
CAPITULO XVII

INSTRUCCIONES SOBRE SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS EN LAS ORGANIZACIONES VIGILADAS

1. CONSIDERACIONES GENERALES

Las organizaciones deben adoptar una política de buenas prácticas en materia de seguridad de la información, que les permita identificar los riesgos operativos tecnológicos, así como la posible materialización de incidentes de seguridad que pongan en riesgo la confidencialidad, integridad y disponibilidad de los activos de información, y se adopten, de manera preventiva, los mecanismos que minimicen su impacto, como un elemento que fortalezca la confianza de las entidades que conforman el sector solidario actual.

2. AMBITO DE APLICACIÓN

Las instrucciones de que trata el presente documento, deben ser aplicadas por las cooperativas especializadas en ahorro y crédito y multiactivas e integrales con sección de ahorro y crédito vigiladas y podrá ser adoptado por las demás organizaciones solidarias supervisadas, teniendo en cuenta su tamaño, características y volumen de operaciones, como una práctica adecuada en busca de la seguridad de la información que manejan.

3. DEFINICIONES

Para efectos de la presente Norma, se establecen las siguientes definiciones:

3.1. **Acción resolutiva:** Acción tomada para evitar la repetición de un incumplimiento mediante la identificación y tratamiento de las causas que la provocaron.

3.2. **Activo de información:** Conocimiento o datos que tienen valor para la organización o el individuo.

3.3. **Amenaza:** Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.

3.4. **Confidencialidad:** Considera que la información no se pone a disposición ni se revela a personal o a entidades no autorizadas.

3.5. **Control:** Medida o acción que modifica un riesgo para prevenir su materialización.

3.6. **Disponibilidad:** Posibilidad de que la información debe estar accesible en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

3.7. **Gobierno de seguridad de la información:** Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas.

3.8. **Integridad:** La información debe ser precisa, coherente y completa desde su creación hasta su destrucción, debe ser inalterada ante accidentes o intentos maliciosos, siempre se debe prevenir modificaciones no autorizadas de la información

3.9. **Nivel de riesgo:** Evaluación del riesgo identificando su posible materialización frente al impacto y probabilidad de ocurrencia.

3.10. **Probabilidad:** Posibilidad del riesgo que se pueda materializar frente a un incidente de seguridad de la información.

3.11. **Políticas de seguridad:** Conjunto de directrices, lineamientos y reglas que permiten velar porque se resguarden los activos de información, aprobados por el consejo de administración.

3.12. **Riesgo residual:** Es el riesgo que queda después del aplicar los controles al riesgo identificado.

3.13. **Seguridad de la información:** Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad

3.14. **Servicios de computación en la nube:** Modelo para permitir un acceso de red conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o proveedor de servicios.

3.15. **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas.

4. ELEMENTOS CLAVE DEL DE LA INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION

4.1. Gobierno de seguridad de la información

La organización vigilada debe definir y poner en marcha el sistema de seguridad de la información como un componente integral de sus prácticas de buen gobierno. El sistema de seguridad de la información proporciona la dirección estratégica a las actividades de seguridad y garantiza que se alcancen los objetivos y que se realice la debida gestión de los riesgos relacionados con seguridad de la información; igualmente establece que los recursos de información de la organización solidaria se utilicen con responsabilidad. Esta es una responsabilidad del consejo de administración o del órgano que haga sus veces y la alta dirección de la organización solidaria.

4.1.1.Estrategia de Seguridad

El objetivo de la estrategia de seguridad de la información es alcanzar el estado deseado definido por los atributos de seguridad de la información en la organización. El plan o planes de acción deben ser formulados sobre la base de los recursos y limitaciones disponibles, incluida la consideración de los requisitos legales y reglamentarios pertinentes.

La organización vigilada debe definir y documentar una política de seguridad de la información, alineada con la estrategia del negocio, que identifique, como mínimo:

a) qué se va a hacer;
b) qué recursos se requerirán;
c) quién será el responsable;
d) cuando finalizará;
e) cómo se evaluarán los resultados logrados

4.1.2.Roles y responsabilidades

La administración y el consejo de administración u órgano, que haga sus veces en la organización solidaria, serán quienes aprueben la política de seguridad de la información y son los responsables de dar cumplimiento a las autorizaciones de sus modificaciones, considerando y llevando a cabo, como mínimo, las siguientes actividades:

4.1.2.1. Consejo de Administración u órgano que haga sus veces

a) Definir y promover la dirección estratégica para la seguridad de la información.
b) Proporcionar los recursos para la adecuada implementación de la seguridad de la información.
c) Proporcionar, velar y apoyar la implementación y asignación del Sistema de Seguridad de Información.
d) Autorizar, facilitar e integrar la puesta en operación del sistema de seguridad de la información, mediante la definición de mecanismos y la supervisión e integración por parte de cada líder de proceso.
e) Supervisar el cumplimiento de las obligaciones regulatorias en materia de seguridad de la información.
f) Velar por la disponibilidad de los recursos y su uso apropiado.
g) Designar los responsables de la implementación del sistema de seguridad de la información.
h) Pronunciarse y hacer seguimiento a los informes trimestrales que presente el representante legal, dejando constancia en las actas de las reuniones respectivas.
i) Aprobar las evaluaciones de riesgo de seguridad de la información resultantes.
j) Revisar que la estrategia de seguridad de la información se encuentre alineada con los objetivos de negocio.
k) Revisar y aprobar las actualizaciones al Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar su continua conveniencia, idoneidad y efectividad.
l) Establecer las prioridades de los proyectos e iniciativas relacionadas con la seguridad de la información.

4.1.2.2. Representante Legal

a) Definir los objetivos estratégicos para la seguridad de la información.

b) Velar por la implementación de la política de seguridad de la información.
c) Facilitar la integración entre los diferentes dueños de procesos de negocio para lograr la implementación del modelo de seguridad de la información.
d) Velar por la disponibilidad de los recursos y su uso apropiado.
e) Velar por la correcta aplicación de los controles de seguridad para reducir el riesgo de seguridad de la información
f) Designar las áreas o cargos que actuarán como responsables de la implementación de la política de seguridad de la información.
g) Presentar un informe periódico, como mínimo trimestral, al Consejo de Administración sobre la evolución y aspectos relevantes de la seguridad de la información incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar, seguimiento y resultados de mediciones y cumplimiento de objetivos de seguridad de la información.

4.1.2.3. Auditoría interna o quien ejerza control interno

Sin perjuicio de las funciones asignadas en otras disposiciones a la auditoría interna, o quien ejerza el control interno, ésta debe:

a) Tener conocimiento apropiado en materia de seguridad de la información y de esta normativa en particular[1].
b) Evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos clave del modelo de seguridad de la información, con el fin de determinar las deficiencias y sus posibles soluciones.
c) Informar los resultados de la evaluación de los responsables de la seguridad de la información.

4.1.3. Estándar base para adaptar el Sistema de Seguridad de la Información

Las organizaciones vigiladas deben adoptar un Modelo de Seguridad y Privacidad de la Información, que permita el aseguramiento de los activos de información y que contemple elementos para establecer, implementar, mantener y proveer mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Para tal efecto, se recomienda tomar como referencia el estándar de seguridad de la información ISO27001 de 2013.

4.2. Riesgos de seguridad de la información

La gestión de riesgos es un proceso encaminado a minimizar las vulnerabilidades y posibles pérdidas de información que pueden llegar a materializarse y afectar económicamente a las organizaciones. Para tal efecto, se deben establecer niveles aceptables de aseguramiento y previsibilidad sobre los resultados deseados de cualquier actividad importante de la organización y llevar a cabo un proceso sistemático que permita:

a) Tener comprensión de las amenazas, las vulnerabilidades, y el perfil de riesgo de la organización.
b) Tener entendimiento de la exposición al riesgo y las posibles consecuencias para el negocio.
c) Crear conciencia de las prioridades de la gestión de riesgos con base en las posibles consecuencias de materialización.

[1] Norma ISO 27001

d) Definir e implementar estrategias organizacionales adecuadas para la mitigación de riesgos para obtener consecuencias aceptables.
e) Fijar la atención organizacional con base en un entendimiento de las posibles consecuencias del riesgo residual.
f) Conservar información documentada del proceso de gestión de riesgos de seguridad de la información.

4.3. Sistema de Seguridad de la información

Las organizaciones solidarias vigiladas deberán contar con políticas que identifiquen el contexto y los objetivos propios de la Entidad, atendiendo como mínimo lo siguiente:

4.3.1. Descripción

El proceso de descripción de las políticas de seguridad de la información, implica que bajo un lenguaje conciso y de fácil comprensión, se identifiquen e incorporen los temas propios de seguridad, normativa aplicable, tipo de información sensible, identificación de la clasificación de la información, responsables y niveles de autorización.

4.3.2. Revisión

El proceso de revisión debe contemplar la aplicación de actividades de retroalimentación como soporte de conocimiento que permitan la socialización y la verificación del cumplimiento de las políticas de seguridad, alineadas con los objetivos de la organización solidaria.

4.3.3. Aprobación

Este proceso está a cargo del consejo de administración o, quien haga sus veces, en la entidad, quien emitirá la aprobación de las políticas del Sistema de Seguridad de Información y establecerá las instrucciones para su puesta en marcha y cumplimiento.

4.3.4. Publicación

Cumplidos los procesos de descripción, revisión y aprobación, la organización vigilada dará a conocer las políticas de seguridad de la información, las cuales deberán ser publicadas a través de los medios de comunicación que habitualmente utiliza, siendo necesario que se apliquen estrategias que faciliten su difusión y su contenido por todos y cada uno de los integrantes de las organizaciones.

4.3.5. Evaluación

La organización solidaria deberá aplicar evaluaciones de conocimiento al personal, garantizando que las políticas son leídas y se aplican de acuerdo a lo establecido.

4.3.6. Actualización

El desarrollo de la Seguridad de Información debe considerarse como un proceso de mejora continua, por lo cual, al aplicar los controles de seguridad bajo parámetros previamente establecidos para su medición, debe generar como resultado los aspectos a corregir, los cambios que se deben realizar o, la identificación de nuevos riesgos.

De igual forma, el resultado de las evaluaciones y verificaciones que evidencien el recurrente incumplimiento a las políticas, la recepción de sugerencias por las partes interesadas y la oportunidad de cambios tecnológicos al interior de la organización solidaria, le permitirán a esta tomar decisión en relación con la necesidad de llevar a cabo procesos de actualización de dichas políticas.

4.4. Recursos

La organización vigilada debe determinar y proporcionar los recursos necesarios para el establecimiento e implementación del Sistema de Seguridad de la Información, que considere los siguientes aspectos:

4.4.1.Presupuesto

El presupuesto deberá contemplar la criticidad de los activos de información involucrados, y los recursos que aseguren la función de seguridad de la información, las herramientas tecnológicas que apoyen a la protección de los activos de información y el proceso de mejora continua.

4.4.2.Competencia

La organización vigilada debe procurar que los responsables de la seguridad de la información cuenten con la competencia necesaria para gestionar los riesgos asociados, evaluar la eficacia de las acciones tomadas y garantizar la información documentada.

4.4.3.Comunicación

La comunicación es especialmente importante entre todas las partes interesadas dentro de las cadenas de suministro, por lo que el Sistema de Seguridad de Información debe proporcionar un medio para comunicar los requisitos exigidos, entre los responsables de la entrega de productos y servicios esenciales de la organización.

4.5. Información documentada

El modelo de seguridad de la información de la organización vigilada debe incluir la información documentada requerida por esta norma, considerando los siguientes componentes:

4.5.1.Principios de seguridad de la información

El consejo de administración tiene la responsabilidad de aprobar una política general de seguridad de la información, la cual debe estar disponible para ser entregada a los organismos de vigilancia y control, teniendo en cuenta que:

a) Esté adecuada al propósito de la organización vigilada.
b) Incluya objetivos de seguridad de la información o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información.
c) Incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información.
d) Incluya el compromiso de mejora continua del sistema de seguridad de la información.
e) Esté disponible como información documentada.

f) Se comunique dentro de la organización vigilada.
g) Esté disponible para las partes interesadas, según sea apropiado.

4.5.2. Otra información documentada

El modelo de seguridad de la información de la organización vigilada, debe estar acompañado por otro tipo de información documentada como:

a) Procedimientos de seguridad.
b) Instructivos o guías técnicas.

4.5.3. Creación y actualización de la información documentada

Cuando se crea y actualiza información documentada del sistema de seguridad, la organización vigilada debe asegurarse de que sea apropiado e incluya:

a) La identificación y descripción[2]
b) El formato[3] y sus medios de soporte[4]
b) La revisión y aprobación con respecto a la idoneidad y adecuación.

4.5.4. Control de la información documentada

La información documentada requerida por el sistema de seguridad de la información, se debe controlar para asegurarse de que esté disponible, adecuada para su uso y esté protegida adecuadamente, entre otros, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad.

El control debe efectuarse sobre la distribución, acceso, recuperación y uso de almacenamiento y preservación, incluida la preservación de la legibilidad, control de cambios, retención y disposición.

5. ETAPAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACION

5.1. Roles y Responsabilidades

La organización debe tener una clara definición de los roles y responsabilidades asignadas a funcionarios acorde a las funciones del cargo. Cada rol debe tener responsabilidad específica con respecto al riesgo y la seguridad de la información.

5.2. Recursos humanos

Las organizaciones deben tener definidos claramente los términos y condiciones de los cargos asociados a la seguridad de la información entre profesionales de la seguridad, los administradores de redes / sistemas de TI, los gerentes, los auditores y los trabajadores en general, respecto a las funciones y responsabilidades en la seguridad de la información.

[2] por ejemplo: título, fecha, autor o número de referencia
[3] versión del software, gráficos
[4] por ejemplo: papel, electrónico

Adicionalmente, es conveniente contar con un programa de concientización/educación sobre la seguridad de la información extendido a directivos y trabajadores, para lo cual será necesario:

a. Proveer toda la información a los funcionarios sobre la postura, estrategias y políticas de seguridad de la información de la organización.

b. Implementar un proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial, por parte de los trabajadores, el cual deberá ser informado a estos desde el proceso de inducción.

c. Se deberán tener en cuenta las promociones, degradaciones, cambios de roles, nuevas responsabilidades, nuevas prácticas de trabajo, renuncias y despidos.

6. REQUERIMIENTOS DE MEDIOS TECNOLÓGICOS Y SEGURIDAD DE LA INFORMACIÓN

En desarrollo de los criterios de seguridad para los medios tecnológicos y considerando los canales de distribución utilizados, las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:

a) Disponer de hardware, software y equipos de telecomunicaciones que mitiguen las amenazas del sector, y crear procedimientos y controles necesarios que permitan la prestación de los servicios y el manejo de la información, en condiciones de seguridad y calidad.
b) Gestionar la seguridad de la información bajo un Modelo de Seguridad y Privacidad de la Información.
c) Gestionar con sus tarjetahabientes seguros sobre los estándares de seguridad como con PCI-DSS[5].
d) Gestionar mecanismos para el envío de información a sus clientes, tales como: certificaciones, extractos, notificaciones, sobreflex, entre otros, así como los medios (tarjetas débito y crédito, chequeras, etc.) bajo medidas de seguridad. Cuando la información que la entidad remite a sus clientes sea de carácter confidencial y se envíe como parte o adjunta a un correo electrónico, ésta deberá estar cifrada.
e) Garantizar, de manera segura, el registro las direcciones IP[6] y los números de los teléfonos fijos y móviles desde los cuales operará. La entidad podrá determinar los procedimientos que permitan identificar y, de ser necesario, bloquear las transacciones provenientes de direcciones IP o números fijos o móviles considerados como inseguros.
f) Todas las conexiones a aplicaciones de terceros deben estar en mecanismos seguros de conexión como son VPN[7], canales exclusivos, con el registro de IP por parte de

5 Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago *(*Payment Card Industry Data Security Standard – *PCI DSS)*

6 IP o Internet Protocol (Protocolo de Internet), es el sistema estándar mediante el cual funciona la internet, por medio de un proceso de envío y recepción de información.

7 Una VPN (sigla en inglés para red privada virtual) es una tecnología que utiliza Internet para conectarse a una ubicación específica y de esta manera poder acceder a ciertos servicios.

entidades para evitar acceder desde lugares remotos sin la debida seguridad y/o autorización pertinente.

6.1. Controles criptográficos

a) Los sitios web creados para el procesamiento de la información del negocio, deben ser sitios seguros y utilizar certificados digitales emitidos por un ente certificador legalmente constituido en el país.
b) Las comunicaciones con terceras partes para la prestación de servicios del negocio, deben utilizar mecanismos de encriptación fuertes.
c) Se deben utilizar herramientas que utilizan algoritmos de encriptación en el almacenamiento de la información sensible o crítica en archivos, así como las claves de usuarios a los sistemas de información.

6.2. Protección contra códigos móviles o maliciosos

a) Se debe mantener instalado, en los equipos de la organización, software antivirus los cuales serán actualizados constantemente por parte del área encargada.
b) Evitar o restringir el intercambio de CD´s, memorias tipo USB y otros medios removibles de origen desconocido o, si fuere necesario, someterlos a la revisión del antivirus instalado en el disco antes de su utilización.
c) Restringir el uso de los equipos por parte de personas ajenas a las actividades propias de la organización.
d) En el caso de los archivos comprimidos bajo el formato ZIP o cualquier otro tipo de archivo que fueron descargados por Internet o por correo electrónico, deberán ser revisados por el antivirus inmediatamente después de haber sido desempaquetados y antes de ser ejecutados.

6.3. Intercambio de información

a) No estará permitido intercambiar información con entidades externas sin la debida autorización y/o acuerdos de confidencialidad que garantice los tratamientos de información pertinentes.
b) Cuando se envié información sensible por correo electrónico, se debe colocar clave a los archivos adjuntos y está debe ser informada al destinatario por un medio diferente al correo electrónico.
c) Los empleados de las entidades y de las empresas aliadas deben estar cubiertas con acuerdos de confidencialidad y, por lo tanto, serán responsables de la entrega de información no autorizada.
d) En caso de ser necesario el envío y la recepción de información confidencial con los terceros contratados, se debe proteger con mecanismos de cifrado fuerte.
e) La información sensible disponible al público a través de sitios web, debe estar protegida por sitios seguros y, adicionalmente, con usuario y clave de acceso.
f) La comunicación con entidades externas para el intercambio de información crítica se debe hacer a través de canales dedicados, con mecanismos de seguridad, como son VPN o webservices y debe ser configurado por personal de la entidad solidaria.
g) La información que viaja entre las oficinas y los sitios centrales de las entidades, deberá estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores. Para los Establecimientos de Crédito, el hardware o software empleados deberán ser totalmente separados e independientes de cualquier

otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se deberá emplear cifrado fuerte. Las entidades deberán evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.

h) Es responsabilidad de los dueños de la información crítica no dejar copias impresas o documentos físicos en lugares de fácil acceso a personal no autorizado.
i) En los contratos o acuerdos de servicios se incluyen los requisitos y condiciones requeridas para el intercambio de información.

6.4. Respaldo de la información

A toda la información que se encuentra alojada en los servidores y equipos de cómputo, se le debe garantizar respaldo periódicamente de acuerdo con los procedimientos establecidos, con el fin de contar con la información en caso de ser requerida por alguna eventualidad y se tendrá en cuenta que:.

a) Las copias de seguridad deben estar enfocadas a los datos, sistemas y programas, servidores, equipos de escritorio, portátiles, red, sistemas de control, sistemas de seguridad, entre otros.
b) Debe garantizar que los medios de respaldo están físicamente protegidos / asegurados al menos al mismo nivel que los datos operacionales.
c) Las copias de seguridad se deben almacenar en ubicaciones adecuadas, protegidos contra desastres físicos y acceso indebido.
d) Se debe implementar un procedimiento para probar, de forma regular, las copias generadas y así garantizar su integridad y funcionalidad al momento de una restauración.

6.5. Sincronización de Relojes

Todos los equipos tanto, servidores, switches, equipos de cómputo, circuito cerrado de cámaras de vigilancia - CCTV, y todos aquellos dispositivos tecnológicos que se tienen en la organización se deben sincronizar a la hora legal colombiana, sin excepción alguna. Se debe garantizar, por medio de seguimiento y con el respectivo indicador, el cumplimiento de la correcta sincronización de la hora según lo expuesto en el numeral 14, del artículo 6, del Decreto 4175 de 2011, con apoyo del Instituto Nacional de Metrología de Colombia (www.inm.gov.co, opción hora legal).

6.6. Controles de Acceso

Se aplica a todas las formas de acceso a las instalaciones de la organización y para aquellas áreas definidas como “áreas críticas”, debido a su relación con datos confidenciales y de interés para el negocio, así:

a) El acceso a las instalaciones que opten por el uso de aplicaciones por medio de software de control de acceso biométrico o tarjeta, debe definir sus responsables y el debido tratamiento de datos personales, conforme a lo dispuesto en la Ley 1581 del 2012, la cual trata del uso de datos sensibles según su clasificación.

b) El acceso de todo el personal (incluyendo contratistas y visitantes) a los Datacenter y Centros de Cableado, debe estar restringido y sólo pueden acceder a través de la autorización correspondiente funcionario.
c) Para preservar la seguridad de los equipos de los servidores y equipos de comunicaciones y, en general, todos los dispositivos de los Datacenters y centros de cableado los armarios (Racks), deben permanecer cerrados.
d) Si se requiere el uso de cámaras de video (CCTV) u otros mecanismos de control de acceso (proximidad o control de acceso biométrico) para supervisar el acceso físico de personas a áreas críticas o que resguardan información confidencial, deben generar su respectivo procedimiento de tratamiento de copias de seguridad a menos que la ley u otras regulaciones requieran un tiempo superior de custodia.
e) Se deben implementar controles físicos que impidan el acceso a conexiones o puntos de red de acceso público. Esto incluye limitar el acceso físico a los puntos de acceso inalámbricos, dispositivos de telecomunicaciones, manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones.

6.7. Tele-Trabajo

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización. Esto incluye el uso de teléfonos móviles, tabletas y similares fuera de las instalaciones de la organización, por lo cual:

a) El acceso remoto a los servidores que se encuentran fuera de las instalaciones de la organización, debe estar autorizado por el comité de riesgos de la entidad o quien delegue la gerencia general.
b) Las áreas de trabajo remoto que autorice la organización fuera de su sede principal, deben cumplir con todas las políticas y controles del sistema de seguridad definido para proteger la información que viaje en ellos.
c) El personal de infraestructura de informática y tecnología son responsables de proporcionar el servicio de acceso

6.8. Acceso a las redes WIFI

a) El acceso a las redes inalámbricas por parte de los empleados, a través de WiFi, se debe realizar con autenticación usuario y contraseña, independientemente de la herramienta que se quiera utilizar para controlar el acceso.
b) Las redes WiFi para clientes o visitantes se debe realizar mediante accesos independientes y por redes lógicas independientes a las redes corporativas.

6.9. Aspectos no permitidos

Los aspectos no permitidos deben quedar contenidos en políticas, principios o procedimientos, manuales y ser de conocimiento por todos los funcionarios de la entidad, entre ellos:

a) Transmisión de contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante o acosador, sea este material o mensajes.

b) Interceptar, recopilar o almacenar datos sobre terceros sin su conocimiento o consentimiento.
c) Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.
d) Enviar mensajes no solicitados (spam), virus, o ataques internos o externos.
e) Obtener acceso no autorizado a equipos, sistemas o programas, tanto al interior de la red como fuera de ella. Tampoco se podrá utilizar la red WIFI para obtener, manipular y compartir cualquier archivo de tipo musical o filmográfico, sin tener los derechos de propiedad intelectual.
f) Dañar equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red. Ser usada con fines de lucro, actividades comerciales o ilegales, por ejemplo, hacking. Ser utilizada para crear y/o la colocar un virus informático o malware en la red.
g) Transmitir, copiar y/o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil, material amenazante u obsceno o material protegido por secreto comercial o patentes.

6.10. Prestación de servicios por terceras partes

Cuando la entidad requiera la contratación de prestación de servicios por terceras partes debe, como mínimo:

a) Firmar el documento de acuerdo de confidencialidad antes de iniciar la prestación del servicio.
b) Elaborar los contratos o acuerdos de prestación de servicios donde se especifiquen claramente las condiciones.
c) Cuando existan cambios en los servicios que prestan las terceras partes, estos deben ser documentados e incluidos en los acuerdos de servicios o contratos.
d) La organización realizará auditorías a las terceras partes para evaluar la seguridad de la información y, como mínimo, se evaluarán integridad, disponibilidad, confidencialidad y calidad del servicio.

6.11. Gestión de Incidentes de Seguridad

Un incidente de Seguridad Informática se define como un evento que atente contra la confidencialidad, integridad y/o disponibilidad de la información y los recursos tecnológicos de la entidad.

Existen varias categorías de incidentes de seguridad que se pueden llegar a presentar, dentro de las cuales se encuentran:

a) Acceso no autorizado: Comprende todo tipo de ingreso y operación no autorizado a los sistemas, tanto exitosos como no exitosos. Son parte de esta categoría:
- Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.
- Robo de información
- Borrado de información
- Alteración de la información
- Intentos recurrentes y no recurrentes de acceso no autorizado

- Abuso y/o Mal uso de los servicios informáticos internos o externos que requieren autenticación

b) Código malicioso: Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica de la Entidad. Son parte de esta categoría:

- Virus informáticos
- Troyanos
- Gusanos informáticos

c) Denegación del servicio: Esta categoría incluye los eventos que ocasionan pérdida de un servicio en particular. Los síntomas para detectar un incidente de esta categoría son:

- Tiempos de respuesta muy bajos sin razones aparentes.
- Servicio(s) interno(s) inaccesibles sin razones aparentes
- Servicio(s) Externo(s) inaccesibles sin razones aparentes

d) Escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular. Esta categoría agrupa los eventos que buscan obtener información de la infraestructura tecnológica de la Entidad y comprende:

- Sniffers (software utilizado para capturar información que viaja por la red)
- Detección de Vulnerabilidades

e) Mal uso de los recursos tecnológicos: Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso y comprende:

- Mal uso y/o Abuso de servicios informáticos internos o externos
- Violación de las normas de acceso a Internet
- Mal uso y/o Abuso del correo electrónico de la Entidad
- Violación de las Políticas, Normas y Procedimientos de Seguridad Informática reglamentadas

Es deber de todas las entidades reportar un incidente de seguridad tan pronto lo detecte o sospeche de el. Para el reporte de un incidente de seguridad, se debe realizar de acuerdo al procedimiento definido por la entidad. Adicionalmente, si estos desencadenan en fraudes para la entidad se deben poner en contacto con las entidades encargadas para la investigación y sanción de estos hechos denominados delitos informáticos, así como su respectivo reporte a la Superintendencia de la Economía Solidaria.

6.12. Divulgación de Información

Diseñar procedimientos para dar a conocer a los clientes, usuarios y funcionarios, los riesgos derivados del uso de los diferentes medios y canales.

6.13. Inventario de activos

Las entidades deberán contar con un inventario de activos de la información, especificando, como mínimo, los siguientes aspectos:

- Datos digitales
- Información impresa
- Software
- Infraestructura
- Servicios de información y proveedores de servicios
- Seguridad física
- Relaciones comerciales
- Responsables de los activos.

Se deben identificar los activos asociados con información e instalaciones de procesamiento de información.

Así mismo, se deberá contar con un proceso y procedimiento detallado para mantener el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo / personal, nuevos sistemas, negocios y cambios de TI.

6.14. Cajeros Automáticos (ATM)

Los cajeros automáticos deberán cumplir, como mínimo, con los siguientes requerimientos:

a) Contar con sistemas de video grabación que asocien los datos y las imágenes de cada transacción. Las imágenes deberán ser conservadas, por lo menos un (1) año o, en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.
b) Cuando el cajero automático no se encuentre físicamente conectado a una oficina, la información que viaja entre este y su respectivo sitio central de procesamiento se deberá proteger utilizando cifrado fuerte, empleando para ello hardware de propósito específico independiente. Las entidades deberán evaluar con regularidad la efectividad y vigencia del mecanismo de cifrado adoptado.
c) Los dispositivos utilizados para la autenticación del cliente o usuario en el cajero deben emplear cifrado.
d) Implementar el intercambio dinámico de llaves entre los sistemas de cifrado, con la frecuencia necesaria para dotar de seguridad a las operaciones realizadas.
e) Los sitios donde se instalen los cajeros automáticos deberán contar con las medidas de seguridad físicas para su operación y estar acordes con las especificaciones del fabricante. Adicionalmente, deben tener mecanismos que garanticen la privacidad en la realización de transacciones para que la información usada en ellas no quede a la vista de terceros.
f) Implementar mecanismos de autenticación que permitan confirmar que el cajero es un equipo autorizado dentro de la red de la entidad.

6.15. POS[8] (incluye PIN Pad[9])

Los POS deberán cumplir, como mínimo, con los siguientes requerimientos:

a) La lectura de tarjetas solo se deberá hacer a través de la lectora de los datáfonos y los PIN Pad cumpliendo con los estándares PCI-DSS.
b) Los administradores de tecnología son los responsables de validar automáticamente la autenticación del datáfono que se intenta conectar a ellos, así como garantizar que los canales de comunicación se encuentren con los debidos controles criptográficos descritos en el presente documento.
c) Establecer procedimientos que le permitan identificar los responsables de los datáfonos en los establecimientos comerciales y confirmar la identidad de los funcionarios autorizados para retirar o hacerles mantenimiento a los equipos.
d) Velar porque la información confidencial de los clientes y usuarios no sea almacenada o retenida en el lugar en donde los POS estén siendo utilizados reduciendo la posibilidad reduzcan la posibilidad de que terceros puedan ver la clave digitada por el cliente o usuario.

6.16. Centro de Atención Telefónica (Call Center, Contact Center)

Los Centros de Atención Telefónica deberán cumplir, como mínimo, con los siguientes requerimientos dando cumplimiento al tratamiento de datos personales, según lo establecido en la Ley 1581 del 2012:

a) Destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada.
b) Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.
c) Garantizar que los equipos destinados a los centros de atención telefónica solo serán utilizados en la prestación de servicios por ese canal.
d) En los equipos usados en los Centros de Atención Telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. Estos registros deberán ser conservados, por lo menos un (1) año o, en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

6.17. Transacciones por Internet

Las entidades que ofrezcan la realización de operaciones por Internet deberán cumplir como mínimo lo siguiente:

[8] El sistema POS es una agrupación de diferentes software y hardware que, al combinarse, permiten a las empresas procesar sus transacciones de cara al cliente.
[9] Un PIN pad o dispositivo de entrada de PIN es un dispositivo electrónico utilizado en una transacción de débito, crédito o tarjeta inteligente para aceptar y cifrar el número de identificación personal del titular de la tarjeta.

a) Implementar los controles descritos en los algoritmos y protocolos necesarios para brindar una comunicación segura.
b) Realizar, como mínimo dos (2) veces al año, una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de transacciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional, esto debe ir acompañado de su respectivo documento de control de cambios.
c) Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus transacciones pueda ser capturada por terceros no autorizados durante cada sesión.
d) Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
e) Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.
f) Implementar mecanismos que permitan a la entidad verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS[10].

6.18. Análisis de Vulnerabilidades

Las entidades deberán implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes aspectos:

a) Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.
b) Generar, de manera automática, por lo menos dos (2) veces al año, un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos (2) años deben contener sus planes de acción y sus remediaciones.
c) Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.
d) Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilitis and Exposures) y actualizadas a la fecha de su utilización.
e) Los informes generados deberán tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).

6.19. Seguridad física y del entorno.

La entidad debe implementar una política para prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización. Para ello, la política debe contemplar, como mínimo:

a) Estudio acerca de si las instalaciones se encuentran en una zona de riesgo.

[10] El Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space) consiste en resolver las peticiones de asignación de nombres.

b) Se definan los perímetros de seguridad (edificios, oficinas, redes informáticas, habitaciones, armarios de red, archivos, salas de máquinas, etc.).
c) Tipo de construcción, en la cual se ubican los activos informativos de la entidad especificando la seguridad con la que cuentan el techo, el exterior, las paredes, el suelo, las ventanas, las puertas y cualquier acceso físico a la ubicación de los equipos que contienen la información.
d) Controles físicos a todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado.
e) Controles implementados a puertas y ventanas para determinar su nivel de seguridad ante algún tipo de intento de violación.
f) Monitoreo a los puntos de acceso con cámaras.
g) Pruebas programadas al sistema de detección de intrusos de la entidad.

6.20. Instalaciones y suministros

La entidad debe proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. Por lo tanto, deberá contar con lo siguiente:

a) Un sistema de UPS[11] para proporcionar una potencia adecuada, confiable y de alta calidad que cuente con una adecuada para abarcar todos los equipos esenciales durante un período de tiempo suficiente.
b) Un plan de mantenimiento y pruebas para los UPS y generadores.
c) Contar con una red de suministro eléctrico redundante
d) Implementar controles para las pruebas de cambio y así garantizar la no afectación de los sistemas y servicios.
e) Contar con sistemas de aire acondicionado redundantes para controlar entornos con equipos críticos y así contar con una capacidad adecuada de A/C para soportar la carga de calor.
f) Implementar detectores de temperatura.

6.21. Planificación e implementación de la continuidad de la seguridad de la información

La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas. Así mismo, deberá establecer, documentar, implementar y mantener procesos procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información.

De igual forma, la organización debe verificar, a intervalos regulares, los controles de continuidad de la seguridad de la información establecidos e implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas. Por lo tanto, deberá contemplar los siguientes aspectos fundamentales:

a) Determinar los requisitos de continuidad del negocio.
b) Elaborar un plan de continuidad de negocio.

[11] Una UPS (Uninterruptible Power Supply) o sistema de alimentación ininterrumpida, es una fuente de suministro eléctrico que permite brindar energía eléctrica por un tiempo limitado a dispositivos eléctricos/electrónicos en el caso de interrupción eléctrica.

c) Contar con un diseño adecuado de "alta disponibilidad" para sistemas de TI, redes y procesos críticos.
d) Identificar el impacto potencial de los incidentes.
e) Evaluar los planes de continuidad del negocio.
f) Realizar DRP[12] para validar el nivel de respuesta de la entidad ante un incidente.
g) Los planes deberán tener plazos definidos para restaurar servicios tras una interrupción.
h) Los planes deberán contar con la identificación y asignación de responsabilidades, la identificación de pérdidas aceptables, la implementación de procedimientos de recuperación y restauración, la documentación de procedimientos y las pruebas regulares.
i) La planificación de la continuidad deberá ser consistente y debe identificar las prioridades de restauración.
j) Deberá contar con miembros de los equipos de recuperación o gestión de crisis o incidentes, con conocimiento de los planes, estableciendo de forma clara sus roles y responsabilidades.
k) Los controles de seguridad deberán estar adecuados para los sitios de recuperación de desastres remotos.
l) Deberá contar con un método de pruebas del plan de continuidad.
m) Se debe establecer la frecuencia con la que se llevaran a cabo las pruebas.
n) Deberán llevar un registro de evidencias de las pruebas reales efectuadas, junto con sus resultados y planes de mejora.
o) Deberán identificar deficiencias para así remediarlas y posteriormente volverlas a probar hasta que los resultados sean satisfactorios.

6.22. Reutilización o eliminación segura de equipos

La organización debe implementar una política para establecer controles con el propósito de verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.

a) La entidad debe evitar que se revele la información almacenada en equipos y dispositivos tras su reasignación o eliminación, mediante el uso de cifrado fuerte o borrado seguro.
b) Llevar un control y registro de cada uno de los medios que se eliminan.

[12] DRP o Plan de Recuperación de Desastres, es un sistema con el cual las organizaciones se preparan contra posibles desastres de diversa índole que puedan dañar su infraestructura tecnológica.