REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN Y TECNOLOGÍA PARA ENTIDADES ASEGURADORAS

SECCIÓN I

ASPECTOS GENERALES

Artículo 1. (Objeto) El presente Reglamento tiene por objeto establecer los controles de Gestión de Seguridad de la Información y Tecnología para Entidades Aseguradoras.

Artículo 2. (Ámbito de Aplicación) Se encuentran sujetas al ámbito de aplicación del presente Reglamento las Entidades Aseguradoras, en adelante denominadas Entidad(es) Regulada(s).

Artículo 3. (Definiciones) Para la interpretación de los términos empleados en el presente reglamento, se establecen las siguientes definiciones:

1. **Activo de información.** Es cualquier recurso de información que tiene valor para la Entidad Aseguradora y contribuye a sus operaciones y objetivos. Estos activos pueden ser datos, documentos, bases de datos, sistemas de información, software, archivos y otros tipos de información que la organización utiliza en formato físico o digital para desarrollar sus actividades.
2. **Ciberseguridad:** Es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos y/o digitales, el término forma parte del concepto de Seguridad de la Información.
3. **Ciclo de vida de la información:** Es el conjunto de etapas por las que la información atraviesa desde su creación, clasificación, uso, difusión, modificación, almacenamiento, preservación y eliminación.
4. **Confidencialidad de la información:** Es la protección de los datos o información contra accesos no autorizados, asegurando que solo las personas, entidades o procesos con permisos adecuados puedan ver o interactuar con la información sensible, que tiene como objetivo restringir la información solo para personas autorizadas, protegiéndola contra la divulgación no autorizada y el uso indebido.
5. **Disponibilidad de la información:** Es la capacidad de un sistema, red o servicio de proporcionar acceso a datos y recursos a los usuarios autorizados cuando se necesiten.
6. **Integridad de la información:** Es la exactitud y confiabilidad de los datos procesados, transportados o almacenados, esto implica que la información no puede ser modificada o destruida de manera no autorizada ya sea de forma intencional o accidental durante su ciclo de vida.
7. **Logs:** Es un registro o bitácora plasmado en un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema de información, así como el conjunto de cambios que estos han generado en la información, los accesos de usuarios, errores y otros eventos significativos que necesitan ser registrados para fines de monitoreo, análisis y auditoría.
8. **Seguridad de la información:** Es el conjunto de medidas preventivas, correctivas y reactivas que permiten resguardar y proteger la información de la Entidad Regulada contra amenazas, vulnerabilidades, accesos no autorizados, uso, divulgación, interrupción, modificación o destrucción, cuyo objetivo principal es preservar la confidencialidad, integridad y disponibilidad de la información.

9. **Servicios en la nube:** Conjunto de servicios de computación, infraestructuras, plataformas y/o sistemas que proveedores externos alojan y ponen a disposición de la Entidad Regulada a través de Internet. Estos servicios son escalables, flexibles y se pueden acceder desde cualquier lugar con una conexión a Internet.

Artículo 4. (Estructura organizativa interna para la Gestión de la Seguridad de la Información y Tecnología) I. La Entidad Regulada debe establecer su organización interna para el cumplimiento de la Gestión de la Seguridad de la Información y Tecnología.

II. La Entidad Regulada debe designar un responsable que ejerza la función de gestionar la Seguridad de la Información y Tecnología, con conocimientos en la materia, encargado de planear, coordinar y administrar los procesos que involucran la Gestión de la Seguridad de la Información y Tecnología.

III. La Entidad Regulada de acuerdo con su estructura organizacional podrá conformar un Comité de Seguridad de la Información y Tecnología para la toma de decisiones en el marco de la Gestión de la Seguridad de la Información y Tecnología.

Artículo 5. (Gestión de Riesgos de Seguridad de la Información y Tecnología) La Entidad Regulada debe Gestionar los Riesgos de Seguridad de la Información y Tecnología, con el objeto de implementar controles de seguridad de la información, a través de la adopción de una metodología específica, que debe contener al menos los siguientes aspectos:

a. El marco regulatorio de la Entidad Regulada.

b. Identificación, clasificación y valoración de los activos de información.

c. Evaluación de los riesgos, identificando las vulnerabilidades de los activos de información y amenazas a los cuales están expuestos.

d. Valoración de los riesgos, evaluando las posibles consecuencias de la materialización de una amenaza producto de las vulnerabilidades identificadas en los activos de información, en función a la valoración del impacto y probabilidad.

e. Tratamiento de los riesgos, tomando decisiones acerca de las medidas y controles apropiados para mitigar, transferir, aceptar o evitar el riesgo identificado.

f. Identificación de los controles implementados.

Artículo 6. (Elaboración, Revisión y Aprobación de Matrices de Declaración de Estado de Controles y Cronograma de Implementación y/o Actualización gradual de Controles de Seguridad de la Información y Tecnología) En función al análisis, evaluación y tratamiento de riesgos de Seguridad de la Información y Tecnología realizado por la Entidad Regulada y en cumplimiento a los controles dispuestos en el presente Reglamento, la Entidad debe elaborar y revisar el Anexo 1 “Matriz de Declaración de Estado de Controles de Seguridad de la Información y Tecnología para Entidades Aseguradoras” y el Anexo 2 “Cronograma de Implementación y/o Actualización gradual de Controles de la Seguridad de la Información y Tecnología para Entidades Aseguradoras” los cuales deben ser aprobados por al menos un miembro del Directorio, el Responsable de Seguridad de la Información y Tecnología o rol con esas funciones, el Gerente General y Funcionarios Responsables de las áreas de servicios Tecnológicos, de Gestión de Riesgo y propietarios de los activos de información.

Artículo 7. (Plazo para el envío anual de documentación sobre la Gestión de la Seguridad de la Información y Tecnología) La Entidad Regulada debe remitir a la Autoridad de Fiscalización y Control de Pensiones y Seguros (APS) hasta el último día hábil del primer mes de cada año, las matrices de “Declaración de Estado de Controles de Seguridad de la Información y Tecnología para Entidades Aseguradoras” (Anexo 1) y el “Cronograma de Implementación y/o Actualización gradual de Controles de la Seguridad de la Información y Tecnología para Entidades Aseguradoras” con la planificación de actividades para la gestión remitida (Anexo 2), aprobados conforme establece el artículo anterior.

SECCIÓN II

CONTROLES DE SEGURIDAD ORGANIZACIONALES

Artículo 8. (Obligaciones respecto a la Gestión de Seguridad de la Información y Tecnología) I. La Entidad Regulada debe aprobar las acciones requeridas para la Gestión de Seguridad de la Información y Tecnología, acorde a sus productos, servicios y operaciones, entre las cuales se encuentran las siguientes:

a. Aprobar políticas, reglamentos, manuales de funciones para la implementación de los controles de Seguridad de Información y Tecnología y su mejora continua.

b. Aprobar la organización, roles y responsabilidades, incluyendo la difusión y capacitación que contribuyan al conocimiento de los riesgos involucrados.

II. La Entidad Regulada debe tomar las medidas necesarias para implementar los controles de seguridad de la información de forma gradual de acuerdo con sus capacidades, según las disposiciones de este reglamento.

III. La Entidad Regulada debe verificar el buen funcionamiento de los controles de seguridad de información; así como, gestionar los riesgos asociados a la Seguridad de la Información y Tecnología.

Artículo 9. (Política de Seguridad de la Información y Tecnología) I. La Entidad Regulada debe definir un conjunto de políticas y/o directrices para la Seguridad de la Información y Tecnología, que sea aprobada, publicada, comunicada y socializada con los empleados de la Entidad, tales políticas deben estar adecuadas a las características y el contexto propio de la Entidad.

II. Las Políticas de Seguridad de la Información y Tecnología, debe tener enunciados generales respecto a los objetivos y principios para guiar todas las actividades relacionadas con la Seguridad de la Información y Tecnología y con la asignación de responsables, los enunciados generales deben incluir al menos los siguientes aspectos:

a. Control de Accesos.

b. Clasificación de la Información.

c. Respaldo de información.

d. Transferencia de información.

e. Administración de vulnerabilidades técnicas.

f. Ciberseguridad de los servicios informáticos.

g. Gestión de seguridad en los contratos con terceros de servicios de informáticos.

h. Seguridad en las comunicaciones.

i. Protección de datos personales de los asegurados o beneficiarios.

j. Responsabilidades de los propietarios de los activos de Información.

k. Seguridad Física y ambiental.

l. Plan de Contingencias Tecnológicas para la continuidad de las operaciones.

Artículo 10. (Roles y responsabilidades en la Seguridad de la Información y Tecnología) La Entidad Regulada debe establecer los roles y responsabilidades respecto a la Gestión de Seguridad de la Información y Tecnología asignados formalmente, estableciendo lo siguiente:

a. Los mecanismos de protección de los activos de información.

b. Los roles en los procedimientos de Seguridad de la Información y Tecnología.

c. La Gestión de Riesgos de Seguridad de la Información y Tecnología para la toma de decisiones en el tratamiento de riesgos.

d. El uso adecuado de los activos de información.

Artículo 11. (Segregación de funciones) La Entidad Regulada, debe segregar las funciones de Seguridad de la Información y Tecnología en conflicto con áreas de responsabilidad sobre los activos de información, con el objeto de reducir el riesgo de fraude, error o evasión de controles, evaluando las siguientes actividades:

a. Solicitar, aprobar y otorgar accesos.

b. Iniciar, aprobar y ejecutar cambios de software o hardware en producción.

c. Desarrollo y administración del software en producción.

d. Usar aplicaciones y administrar bases de datos.

e. Diseñar, auditar o controlar el cumplimiento e implementación de controles de Seguridad de la Información y Tecnología.

Artículo 12. (Funciones del Responsable de Seguridad de la Información y Tecnología) El Responsable de Seguridad de la Información y Tecnología, tiene las siguientes funciones principales:

a. Analizar, evaluar, proponer y documentar los controles para el tratamiento de los riesgos de Seguridad de la Información y Tecnología.

b. Actualizar y revisar la documentación de los avances del proceso continuo de Gestión de Riesgos de Seguridad de la Información y Tecnología.

c. Elaborar la “Matriz de Declaración de Estado de Controles de Seguridad de la Información y Tecnología para Entidades Aseguradoras” (Anexo 1).

d. Elaborar y coordinar el “Cronograma de Implementación y/o Actualización gradual de Controles de Seguridad de la Información y Tecnología para Entidades Aseguradoras” (Anexo 2).

e. Implementar, revisar y verificar el cumplimiento de los controles establecidos en el presente Reglamento.

f. Gestionar la implementación de normativa interna de Seguridad de la Información y Tecnología.

g. Gestionar los incidentes de Seguridad de la Información y Tecnología.

h. Informar sobre los incidentes de Seguridad de la Información y Tecnología al Directorio de la Entidad Regulada.

i. Informar a la APS en caso de tratarse de un incidente crítico que afecte las operaciones de la Entidad Regulada o comprometa sus activos de información en un plazo máximo de dos (2) días hábiles administrativos.

j. Planificar y ejecutar capacitaciones sobre Seguridad de la Información y Tecnología a todo el personal de la Entidad Regulada.

k. Elaborar un Plan de Contingencias Tecnologías en base a un análisis de impacto de los productos, servicios y operaciones que brinda la Entidad Regulada.

l. Gestionar la Auditoría de cumplimiento cuando corresponda.

m. Mantener y actualizar un inventario de activos de información, para fines del control de Gestión de Seguridad de la Información y Tecnología.

n. Otras a ser asignadas por la Entidad Regulada.

Artículo 13. (Gestión de incidentes de Seguridad de la Información y Tecnología) I. La Entidad Regulada debe planificar y prepararse para la Gestión de Incidentes de Seguridad de la Información y Tecnología, definiendo, estableciendo y comunicando procesos, roles y responsabilidades de Gestión de Incidentes de Seguridad de la Información y Tecnología.

II. El proceso de gestión de incidentes debe incluir al menos los siguientes aspectos:

a. Establecer un procedimiento para informar eventos de Seguridad de la Información y Tecnología.

b. Establecer un proceso de gestión de incidentes para proporcionar a la entidad la capacidad de gestionar incidentes de Seguridad de la Información y Tecnología, incluida la administración, documentación, detección, clasificación, priorización, análisis, comunicación y coordinación con las partes interesadas.

c. Establecer un proceso de respuesta a incidentes para proporcionar a la organización la capacidad de evaluar, responder y aprender de los incidentes de Seguridad de la Información y Tecnología.

d. Adecuada manipulación de evidencias.

e. Uso de formularios de incidentes para ayudar al personal a realizar todas las acciones necesarias al informar incidentes de Seguridad de la Información y Tecnología.

f. Identificar eventos o incidentes ocurridos y sus causas, con el fin de determinar e implementar controles adicionales para reducir la probabilidad o las consecuencias de futuros incidentes similares.

g. Información que reportará, de acuerdo a sus políticas y de manera oportuna, a los asegurados, beneficiarios y usuarios de productos y servicios afectados, sobre incidentes de ciberseguridad que hubiesen afectado la confidencialidad o integridad de su información, así como las medidas adoptadas para mitigar el incidente.

III. La Entidad Regulada debe remitir a la APS, en un plazo máximo de diez (10) días hábiles administrativos después de haber reportado un incidente de seguridad crítico con afectación a sus operaciones, un informe con la documentación respaldatoria que incluya los siguientes aspectos:

a. Fecha y hora de inicio y fin de la ocurrencia.

b. Descripción del incidente.

c. Causas de las fallas.

d. Diagnóstico técnico.

e. Canales y servicios afectados.

f. Tiempo fuera de servicio.

g. Impacto ocasionado.

h. Acciones correctivas ejecutadas y/o plan de acción a implementar por la Entidad Regulada para identificar las causas que originaron el incidente, así como para prevenirlos en el futuro y reparación de los daños ocasionados.

Artículo 14. (Inventario de activos de información) I. La Entidad Regulada debe mantener actualizado un inventario de activos de información con la asignación respectiva de los propietarios de los activos de información, con el objeto de preservar la Seguridad de la Información y Tecnología definida por los mismos.

II. El inventario de activos de información, debe contar con la siguiente información: tipo de activo, formato, clasificación, propietario, valor y custodio.

III. La Entidad Regulada debe documentar el inventario de activos de información y proporcionar la información cuando sea requerido por la APS.

Artículo 15. (Uso aceptable de los activos de información) Las reglas para el uso aceptable y manipulación de información deben ser identificados, documentados e implementados por la Entidad Regulada en función a los requisitos de seguridad que establezcan los propietarios, que incluya:

- **a.** Uso permitido y prohibido de los activos de información durante todo el ciclo de vida de la información.
- **b.** Restricciones de acceso que respalden los requisitos de protección para cada nivel de clasificación de información.
- **c.** Mantener un registro de usuarios autorizados de acceso a los activos de información.
- **d.** Protección de copias temporales o permanentes de la información a un nivel consistente con la información original.
- **e.** Almacenamiento o archivo de la información con los mecanismos adecuados de protección.
- **f.** Autorización para la disposición de activos de información y procedimientos de eliminación segura de la información.
- **g.** Mantener un registro de accesos a información sensible o crítica.
- **h.** Mantener un registro de copias físicas entregadas al personal.

Artículo 16. (Devolución de activos de información) I. El personal y otras partes interesadas de la Entidad Regulada, según corresponda, deben devolver todos los activos de información que estén en su poder al cambiar o terminar su vinculación, contrato o acuerdo.

II. La Entidad Regulada debe identificar y documentar toda la información y otros activos asociados a ser devueltos que debe incluir lo siguiente:

- **a.** Equipos informáticos asignados al personal.
- **b.** Dispositivos de almacenamiento portátil.
- **c.** Hardware de autentificación o dispositivos físicos de acceso.
- **d.** Copias físicas de información.

Artículo 17. (Transmisión de datos o información) La Entidad Regulada debe establecer reglas, procedimientos o acuerdos de transferencia de datos o información para todos los medios de transmisión, internamente y con otras entidades, debiendo incluir lo siguiente:

- **a.** Detección y protección contra malware que puede transmitirse mediante el uso de comunicaciones electrónicas y/o digitales.
- **b.** Protección de la información electrónica y/o digital confidencial comunicada en forma de archivo adjunto.
- **c.** Prevención contra el envío de documentos y mensajes en las comunicaciones a la dirección o número equivocado.
- **d.** Antes de usar servicios públicos externos, como mensajería instantánea, redes sociales, uso compartido de archivos o almacenamiento en la nube.
- **e.** Restricciones y controles en la transferencia de información vía correo electrónico.

f. Prohibir la transferencia de información sensible o confidencial por medios electrónicos y/o digitales personales.

g. Responsabilidades de control y notificación de la transmisión, despacho y recepción de información física.

Artículo 18. (Control de accesos) I. Las reglas para controlar el acceso físico y lógico a los activos de información deben establecerse e implementarse en función de los requisitos de Seguridad de la Información y Tecnología de la Entidad Regulada.

II. Los propietarios de los activos de información deben determinar los requerimientos relacionados al control de acceso, que contemplen lo siguiente:

a. Determinar qué entidades requieren, qué tipo de acceso a la información y otros activos asociados.

b. Seguridad en el acceso de los sistemas o servicios informáticos.

c. Acceso físico, que debe estar respaldado por controles de entrada físicos apropiados.

d. Difusión, autorización, niveles de seguridad y clasificación de la información.

e. Restricciones de acceso de cuentas privilegiadas.

f. Autorización formal de solicitudes de acceso.

g. Controles en el inicio de sesión.

h. Factores de autenticación, a fin de verificar la identidad de un usuario o servicio para el acceso a un sistema, los cuales se relacionan con aspectos de conocimiento, posesión, inherencia, conducta y ubicación.

i. Establecer perfiles de acceso bajo de acuerdo al principio de privilegio mínimo.

j. Establecer la política de que todo acceso está prohibido a no ser que sea expresamente permitido.

k. Uso de canales seguros.

Artículo 19. (Gestión de la identificación de usuarios) I. Debe gestionarse el ciclo de vida completo de la identificación de usuarios, con el objeto de contar con identificación única de las personas y a los sistemas informáticos a los que acceden para permitir la asignación adecuada de derechos de acceso.

El proceso de gestión de identificación de usuarios debe considerar, lo siguiente:

a. Para las identidades asignadas a personas, una identidad específica solo se vincula a una sola persona que será responsable por las acciones realizadas.

b. Las identidades asignadas a varias personas solo se permiten cuando son necesarias por razones operativas en la entidad y están sujetas a aprobación y documentación específica.

c. Las identidades asignadas a entidades no humanas están sujetas a una aprobación apropiadamente segregada y a una supervisión continua independiente.

d. Las identidades deben ser deshabilitadas o eliminadas de manera oportuna si ya no son necesarias.

e. Se deben mantener registros de todos los eventos de Seguridad de la Información y Tecnología relacionados con el uso y la gestión de las identidades de los usuarios y de la información de autenticación.

Artículo 20. (Información de autenticación) I. La asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación (usuario y contraseña).

II. El proceso de asignación y gestión de la información de autenticación debe incluir lo siguiente:

- **a.** La información de autenticación, incluida la que es temporal, se transmite a los usuarios de manera segura y se evita el uso de mensajes de correo electrónico sin protección para este propósito.
- **b.** La información de autenticación predeterminada predefinida o proporcionada por los proveedores se cambia inmediatamente después de la instalación de sistemas o software.
- **c.** La información de autenticación es confidencial y no debe compartirse con ninguna persona.
- **d.** La información de autenticación afectada o comprometida se cambia inmediatamente después de la notificación o cualquier otra indicación de un compromiso.
- **e.** El personal de la Entidad Regulada no podrá utilizar la misma contraseña para servicios y sistemas informáticos ajenos a la entidad.
- **f.** Forzar el uso de contraseñas seguras y establecer un nivel de complejidad.
- **g.** Forzar el cambio de contraseña en la primera autentificación.
- **h.** Forzar el cambio de contraseña por caducidad o por requerimiento posterior a un incidente de Seguridad de la Información y/o Tecnología.
- **i.** Prevenir la reutilización de contraseñas anteriores.
- **j.** No desplegar la contraseña en la pantalla cuando se está autentificando.

Artículo 21. (Derechos de acceso) I. Los derechos de acceso a los activos de información deben proporcionarse, revisarse, modificarse y eliminarse (revocarse) de acuerdo con la política específica de la Entidad Regulada y las reglas para el control de acceso.

II. El proceso para asignar o revocar los derechos de acceso físico y lógico otorgados a los usuarios autenticados, debe incluir:

- **a.** Obtener autorización del propietario del activo de información para el uso o acceso.
- **b.** Garantizar que los derechos de acceso se revoquen cuando alguien no necesite acceder al activo de información, en particular inhabilitar de manera oportuna los derechos de acceso de los usuarios que han dejado la entidad.
- **c.** Aplicar la otorgación de derechos de acceso temporal por un período de tiempo limitado y revocarlos en la fecha de vencimiento.
- **d.** Los derechos de acceso deben activarse solo después de que los procedimientos de autorización se completen con éxito.
- **e.** Mantener un registro central de los derechos de acceso otorgados o revocados a un identificador de usuario (Identificador lógico o físico) para acceder al activo de información.
- **f.** Modificar los derechos de acceso de los usuarios que han cambiado de roles o funciones.
- **g.** Efectuar revisiones regulares de los derechos de acceso físico y lógico por movimiento o baja del personal en la entidad y de la autorización de accesos de cuentas privilegiadas.

Artículo 22. (Seguridad en las relaciones con proveedores) Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de Seguridad de la Información y Tecnología asociados con el uso de los productos o servicios de proveedores, que debe incluir:

a. Definir la información de la organización, los servicios o sistemas informáticos y la infraestructura física a la que los proveedores pueden acceder, monitorear, controlar o utilizar.

b. Cuando concluye la relación con el proveedor, se debe asegurar la revocación de accesos lógicos o físicos y la recepción de toda la información manejada por el proveedor.

c. Suscribir acuerdos de confidencialidad con los proveedores.

d. Obligación de los proveedores de implementar un conjunto de controles acordado, incluido el control de acceso, revisión del desempeño, monitoreo, informes, auditoría y las obligaciones del proveedor de cumplir con los requisitos de Seguridad de la Información y Tecnología.

e. Exigir que los proveedores de servicios de tecnologías de la información y comunicación propaguen los requisitos de seguridad de la organización a lo largo de la cadena de suministro si subcontratan partes del servicio proporcionado a la Entidad Regulada.

f. Seguimiento, revisión y gestión de cambios de servicios de proveedores.

Artículo 23. (Seguridad de la Información y Tecnología para el uso de servicios en la nube) Los procesos de adquisición, uso, gestión y contratación de los servicios en la nube deben efectuarse de acuerdo con los requisitos de Seguridad de la Información y Tecnología de la Entidad Regulada, que incorporen al menos los siguientes aspectos:

a. Requisitos de Seguridad de la Información y Tecnología relevantes asociados con el uso de los servicios en la nube.

b. Criterios de selección del proveedor de servicios en la nube y alcance del uso del servicio.

c. Funciones y responsabilidades relacionadas con el uso y la gestión de los servicios en la nube.

d. Identificar los controles de Seguridad de la Información y Tecnología que son administrados por el proveedor de servicios y cuáles son administrados por la organización, como cliente del servicio en la nube.

e. Cómo obtener y utilizar las capacidades de Seguridad de la Información y Tecnología proporcionadas por el proveedor de servicios en la nube.

f. Procedimientos para el manejo de incidentes de Seguridad de la Información y Tecnología que se produzcan en relación con el uso de servicios en la nube.

g. Establecer acuerdo de nivel de servicio.

h. La Entidad Regulada debe establecer en el contrato, los criterios que garanticen el debido tratamiento y protección de los datos personales cuando se utilicen los servicios en la nube.

i. El proveedor del servicio debe cumplir con la normativa y legislación del Estado Plurinacional de Bolivia.

Artículo 24. (Plan de contingencias tecnológicas) La Entidad Regulada debe contar con un plan de contingencias tecnológicas formalizado e implementado, el cual debe ser actualizado al menos una vez al año, que permita mantener la continuidad de los servicios y sistemas informáticos esenciales y asegurarse de:

a. Contar con una estructura organizativa adecuada para prepararse, mitigar y responder ante una interrupción en los servicios y sistemas informáticos, con el apoyo de personal con la autoridad y competencia necesarias.

b. Realizar un análisis de impacto de negocio, identificando los servicios y sistemas informáticos que apoyan la continuidad de las operaciones de la Entidad Regulada.

c. Establecer por cada servicio o sistema informático, el objetivo de tiempo de recuperación y el objetivo de punto de recuperación.

d. Evaluar periódicamente mediante ejercicios y pruebas, al menos una vez al año los planes de continuidad de los servicios y sistemas informáticos necesarios para la continuidad de las operaciones, evidenciando las pruebas en documentos.

Artículo 25. (Protección de registros - logs) Los registros (logs) deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada, para lo cual la Entidad Regulada debe:

a. Emitir directrices sobre el almacenamiento, el manejo de la cadena de custodia y la eliminación de registros (logs), lo que incluye la prevención de la manipulación de los registros.

b. Los registros (logs) deben clasificarse por tipos de registros como contables, de transacciones comerciales, de personal, de los consumidores de servicios, legales, cada uno con detalles de períodos de retención y tipo de medios de almacenamiento permitidos que pueden ser físicos, electrónicos y/o digitales.

c. Elaborar un programa de retención que defina los registros (logs) y el período de tiempo durante el cual deben conservarse, de acuerdo con la política de seguridad de la información y tecnología que defina la Entidad Regulada por tipo de registro.

d. Se debe registrar y almacenar los registros de forma centralizada, de modo que permita conocer adiciones, modificaciones o eliminaciones, independientemente del origen de la manipulación.

e. Establecer accesos a la consulta de los registros en conformidad con las Políticas de Seguridad de la Información y Tecnología adoptadas por la Entidad Regulada.

Artículo 26. (Privacidad y protección de la información de identificación personal) La Entidad Regulada debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la información de identificación personal del asegurado o beneficiario de acuerdo con la normativa vigente aplicables e incluirlas como requisitos contractuales en sus operaciones con proveedores de servicios, estableciendo e implementando los procedimientos y controles informáticos respectivos.

Artículo 27. (Cumplimiento de políticas, normas y estándares de Seguridad de la Información y Tecnología) **I.** La Entidad Regulada debe revisar periódicamente, el cumplimiento de la política de Seguridad de la Información y Tecnología, las reglas y los estándares específicos de seguridad.

II. La Entidad Regulada debe identificar desviaciones o posibles incumplimientos de los requisitos de Seguridad de la Información y Tecnología definidos en la política, las reglas, los estándares y otras reglamentaciones aplicables de Seguridad de la Información y Tecnología que considere pertinentes.

III. Los resultados de las revisiones y acciones correctivas llevadas a cabo en los sistemas de la Entidad Regulada deben registrarse y estos “logs” deben protegerse contra pérdidas y mantenerse para revisión de la APS.

Artículo 28. (Procedimientos documentados) Se deben elaborar procedimientos para la operación de procesamiento de información y posteriormente poner a conocimiento del personal pertinente:

a. Cuando la actividad debe ser realizada de la misma manera por muchas personas.

b. Cuando la actividad es nueva y presenta un riesgo si no se realiza correctamente.

c. Estableciendo instrucciones de manejo, procedimientos de recuperación y reinicio del sistema, la gestión de la pista de auditoría, procedimientos de control como la capacidad, el rendimiento, la seguridad y las instrucciones de mantenimiento.

Artículo 29. (Designar a propietarios de la información) La Entidad Regulada debe identificar a los Propietarios de la Información y asignar formalmente la responsabilidad de:

a. Definir y establecer los requisitos funcionales, conceptuales y características especializadas de la lógica de funcionamiento para el desarrollo o mantenimiento de los sistemas informáticos de su especialidad.

b. Autorizar los accesos de alta, modificación o revocación a los usuarios de los sistemas y/o módulos asignados a su propiedad.

c. Emitir conformidad de las funcionalidades implementadas en los sistemas o módulos.

d. Capacitar en el uso funcional y de su competencia a los usuarios que lo requieran de los sistemas informáticos de su propiedad.

e. Determinar la inhabilitación de los sistemas informáticos de su propiedad asumiendo la custodia de la copia de respaldo de la información para consulta histórica.

f. Administrar el inventario de los servicios y sistemas informáticos que soportan los servicios y operaciones de la Entidad Regulada.

SECCIÓN III

CONTROLES DE SEGURIDAD RELACIONADOS CON RECURSOS HUMANOS

Artículo 30. (Suscribir acuerdos de confidencialidad, términos y condiciones de Seguridad de la Información y Tecnología) I. Los acuerdos contractuales de trabajo deben establecer las responsabilidades del personal y de la organización para la Seguridad de la Información y Tecnología.

II. Las obligaciones contractuales para el personal deben tener en cuenta la política de Seguridad de la Información y Tecnología de la Entidad Regulada y la normativa específica emitida por la APS, considerando:

a. Acuerdo de confidencialidad o no divulgación, debidamente firmado con el personal antes de darle accesos a la información confidencial y otros activos asociados.

b. Responsabilidad legal, posterior a la desvinculación o cambio de funciones.

c. Responsabilidades para la clasificación de la información y la gestión de la información de la entidad, las instalaciones de procesamiento de información y los servicios de información manejados por el personal.

d. Responsabilidades por el manejo de la información en todo el ciclo de vida de la información.

e. Acciones o sanciones por efectuar en caso de que el personal, no cumpla con los requisitos de seguridad de la Entidad Regulada.

Artículo 31. (Política de escritorio despejado) La Entidad Regulada debe definir y aplicar una política del orden y limpieza en sus espacios de trabajo durante y fuera de las horas de trabajo, estableciendo lo siguiente:

a. Los mecanismos para el resguardo de la información confidencial, datos personales de los asegurados o beneficiarios y la información crítica en papel o en medios de almacenamiento electrónicos y/o digitales.

b. Dejar los equipos de computación de usuario final desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación de usuario cuando estén desatendidos.

c. Las computadoras y sistemas deben configurarse con una función de tiempo de espera o cierre de sesión automático.

d. Almacenar de forma segura documentos y medios de almacenamiento extraíbles que contengan información confidencial y cuando ya no se necesiten, desecharlos mediante mecanismos seguros de eliminación.

e. Establecer reglas para el manejo de la información confidencial en impresoras, fotocopiadoras, pizarras u otros medios.

Artículo 32. (Trabajo remoto) La Entidad Regulada debe implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización, estableciendo:

a. Reglas y mecanismos de seguridad para el entorno físico remoto, sobres con información confidencial, transporte seguro entre ubicaciones y reglas para el acceso remoto, política de escritorio despejado, impresión y eliminación de información e informes de eventos de Seguridad de la Información y Tecnología.

b. Los entornos físicos de trabajo remoto esperados.

c. Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas informáticos de la entidad, la sensibilidad de la información a acceder y pasar por el enlace de comunicación y la sensibilidad de los sistemas y aplicaciones.

d. Una definición del trabajo permitido, la clasificación de la información a la que se puede acceder y los sistemas y servicios internos a los que el trabajador remoto está autorizado en su acceso.

Artículo 33. (Incidentes de Seguridad de la Información y Tecnología) La Entidad Regulada debe proporcionar un mecanismo para que el personal notifique eventos o incidentes de Seguridad de la Información y Tecnología que comprometan la integridad, confidencialidad o disponibilidad de la información en los sistemas de información a través de los canales apropiados de manera oportuna y confidencial. Las situaciones referidas a un posible evento de Seguridad de la Información y Tecnología incluyen:

a. Pérdida de disponibilidad de un servicio o sistema informático.

b. Controles de Seguridad de la Información y Tecnología ineficaces.

c. Incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información.

d. Infracciones de las medidas de seguridad física.

e. Funcionamiento inadecuado u otro comportamiento anómalo del sistema de software, hardware o vulnerabilidades identificadas.

f. Sospecha de infección de malware.

g. Violación en la confidencialidad o integridad de la información.

h. Acceso no autorizado.

i. Exposición de datos personales.

SECCIÓN IV

CONTROLES DE SEGURIDAD TECNOLÓGICOS

Artículo 34. (Dispositivos de los usuarios finales) La Entidad Regulada debe establecer la configuración y el manejo seguro de la información en los dispositivos asignados al usuario final, estableciendo lo siguiente:

a. El tipo de información y el nivel de clasificación que los dispositivos de punto final del usuario pueden manejar, procesar, almacenar o admitir.

b. Requisitos para la protección física del dispositivo.

c. Restricción de instalación de software y actualización.

d. Reglas para la conexión a servicios de información, redes públicas o cualquier otra red fuera de las instalaciones.

e. Protección contra malware.

f. Respaldos de información.

g. El uso de dispositivos extraíbles, incluidos los dispositivos de memoria extraíbles, y la posibilidad de desactivar los puertos físicos.

Artículo 35. (Otorgación de derechos de acceso privilegiado) La Entidad Regulada debe restringir y gestionar, la asignación y el uso de derechos de acceso privilegiado para cada sistema informático, sistemas operativos, sistemas de administración de bases de datos y aplicaciones estableciendo lo siguiente:

a. Identificación de usuarios que necesitan derechos de acceso privilegiado.

b. Asignar derechos de acceso privilegiado a los usuarios según sea necesario de acuerdo con la política de control de acceso y el principio de privilegio mínimo.

c. Contar con la autorización y registro de todos los privilegios asignados como ser altas, bajas y/o modificaciones.

d. Definir e implementar los requisitos para la expiración de los derechos de acceso privilegiado.

e. Registrar todos los accesos de cuentas privilegiadas con fines de auditoría.

f. Deshabilitar las cuentas privilegiadas por defecto.

Artículo 36. (Acceso al código fuente) La Entidad Regulada debe implementar mecanismos para el control estricto al código fuente, documentación del desarrollo e información técnica de las herramientas de desarrollo, debiendo mantener un registro de los accesos (logs) y un repositorio de las versiones del código fuente.

Artículo 37. (Protección contra malware) La Entidad Regulada debe instalar y actualizar regularmente software de detección de malware, con el objeto de escanear los equipos de computación y medios de almacenamiento electrónicos y/o digitales, considerando lo siguiente:

a. La protección contra el malware debe implementarse y respaldarse mediante la capacitación adecuada del usuario.

b. La protección contra el malware debe basarse en software de detección y eliminación de malware, conciencia de Seguridad de la Información y Tecnología, acceso al sistema adecuado y controles de gestión de cambios.

c. Búsqueda exhaustiva de amenazas en archivos adjuntos y descargas de correo electrónico y mensajería instantánea en busca de malware antes de su uso.

d. Actualización del software antimalware contra nuevas amenazas.

Artículo 38. (Gestión de vulnerabilidades técnicas) La Entidad Regulada debe realizar evaluaciones de vulnerabilidades de Seguridad de la Información y Tecnología al menos una vez (1) al año, utilizando técnicas de intrusión y penetración en los sistemas de información en uso, hardware, software o red , para encontrar fallas de seguridad en un entorno controlado, con el propósito de identificar, evaluar y reportar vulnerabilidades, debilidades, deficiencias o fallos técnicos que permitan a usuarios no legítimos obtener accesos no autorizados y llevar a cabo operaciones no permitidas que comprometan la Seguridad de la Información y Tecnología, considerando principalmente los siguientes aspectos:

a. Asegurar la notificación, manejo y divulgación de vulnerabilidades, incluidos los requisitos en los contratos aplicables con proveedores de sistemas de información.

b. Usar herramientas de búsquedas exhaustivas de amenazas para las tecnologías en uso para identificar y verificar si las actualizaciones de software (parches) contra las vulnerabilidades aplicadas fueron exitosas.

c. Realizar pruebas de penetración planificadas, documentadas y repetibles o evaluaciones de vulnerabilidad por parte de personas autorizadas para respaldar la identificación de vulnerabilidades.

d. Detectar la existencia de vulnerabilidades en sus productos y servicios incluyendo cualquier componente externo utilizado en estos y recibir informes de vulnerabilidad de fuentes internas o externas.

Artículo 39. (Gestión de la configuración) La Entidad Regulada debe definir e implementar procesos y procedimientos con herramientas para hacer cumplir las configuraciones de seguridad para hardware, software, servicios en la nube y redes, para sistemas recién instalados, software en uso, así como para sistemas operativos durante su vida útil.

Artículo 40. (Enmascaramiento de datos) La Entidad Regulada debe establecer mecanismos y procedimientos de enmascaramiento de datos, modificando los datos personales de un determinado sistema en ambientes de desarrollo, pruebas y calidad, con el fin de proteger la confidencialidad de la información de los asegurados y beneficiarios.

Artículo 41. (Prevención de fuga de información) La Entidad Regulada debe establecer mecanismos y procedimientos para la prevención de fuga de información, estableciendo lo siguiente:

a. La identificación y clasificación de la información para su protección contra posibles fugas de información.

b. El monitoreo de canales de fuga de información como correo electrónico, transferencias de archivos, almacenamiento en la nube, dispositivos móviles y dispositivos de almacenamiento portátiles.

c. Detecte la divulgación de información confidencial cuando la información se cargue en servicios en la nube de terceros no confiables o se envíe por correo electrónico.

d. Restringir el uso de los servicios de correo electrónico o almacenamiento en la nube de índole personal o ajena a la Entidad Regulada.

Artículo 42. (Copias de Seguridad de la Información y Tecnología) La Entidad Regulada debe efectuar, mantener y probar regularmente, las copias de Seguridad de la Información y Tecnología generadas para el software, sistemas informáticos, bases de datos, información u otro activo de información de acuerdo con la política establecida, que debe incluir al menos lo siguiente:

a. Producir registros precisos y completos de las copias de seguridad y los procedimientos de restauración documentados.

b. Cumplir con los requisitos de los niveles de servicio y de las operaciones de la Entidad Regulada, los requisitos de Seguridad de la Información, punto objetivo de recuperación y Tecnología involucrada y la criticidad de la información para la operación continua de la entidad en el alcance (respaldo completo o diferencial) y la frecuencia de los respaldos.

c. Almacenar de forma ordenada y etiquetada las copias de seguridad en una ubicación segura y protegida del sitio principal.

d. Probar regularmente los medios de respaldo para garantizar que se pueda confiar en ellos para uso de emergencia cuando sea necesario.

e. Mantener en operación los dispositivos necesarios para la restauración de copias de seguridad.

Artículo 43. (Proceso de monitoreo) La Entidad Regulada debe establecer mecanismos y procedimientos de monitoreo en las redes, los sistemas informáticos y las aplicaciones con el fin de detectar comportamientos anómalos y posibles incidentes de Seguridad de la Información y Tecnología, en:

a. Tráfico de red, sistema y aplicación saliente y entrante.

b. Acceso a sistemas, servidores, equipos de red, sistema de monitoreo, aplicaciones críticas.

c. Archivos de configuración de red y sistema de nivel crítico o de administrador.

d. Registros de herramientas de seguridad (antivirus, filtrado web, cortafuegos, prevención de fuga de datos).

e. Uso de los recursos (CPU, discos duros, memoria, ancho de banda) y su rendimiento.

Artículo 44. (Sincronización de tiempo) Los relojes de los sistemas de procesamiento de información utilizados en la Entidad Regulada debe sincronizarse con las fuentes de tiempo aprobadas, para permitir la correlación y el análisis de eventos relacionados con la seguridad y otros datos registrados, que respaldan las investigaciones sobre incidentes de Seguridad de la Información y Tecnología.

Artículo 45. (Uso de programas utilitarios privilegiados) El uso de programas utilitarios que pueden anular los controles de aplicaciones y sistemas debe restringirse y controlarse estrictamente, para garantizar que el uso de los mismos no perjudique los controles de aplicaciones y sistemas para la Seguridad de la Información y Tecnología.

Artículo 46. (Instalación de software en sistemas operativos) La Entidad Regulada debe implementar procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos, para garantizar la integridad de los sistemas operativos y evitar la exposición de vulnerabilidades técnicas, Tales procedimientos deben contemplar los siguientes aspectos:

a. Solo usuarios con perfil administrador pueden realizar actualizaciones de software operativo.

b. Solo instalar y actualizar el software después de pruebas exhaustivas.

c. Usar un sistema de control de configuración para mantener el control de todo el software operativo.

Artículo 47. (Seguridad en redes) La Entidad Regulada debe establecer mecanismos y procedimientos para proteger las redes y los dispositivos de red, considerando lo siguiente:

a. El tipo y nivel de clasificación de la información que la red puede soportar.

b. Establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red.

c. Mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración de los dispositivos (enrutadores, conmutadores, switches, firewalls u otros dispositivos de red).

d. Segmentar en subredes las operaciones de los sistemas informáticos cuando corresponda.

e. Sistemas de autenticación en la red.

f. Sistemas de restricción y filtrado de conexión a la red.

g. El acceso a sitios web externos restringidos debe administrarse a través de herramientas de filtrado web.

h. Implementar medidas de seguridad adicionales en la red para reducir la posibilidad de ataques cibernéticos, así como mejorar su protección para hacerlo resistente a amenazas.

i. Deshabilitar protocolos de red no utilizados

Artículo 48. (Uso de criptografía) I. La Entidad Regulada debe definir e implementar reglas para el uso eficaz de criptografía, incluida la gestión de claves criptográficas, estableciendo responsables de definir contraseñas de cifrado y que corresponde cifrar, para proteger la confidencialidad, autenticidad o integridad de la información, de acuerdo a requisitos comerciales y de Seguridad de la Información y Tecnología, tomando en cuenta el ordenamiento jurídico vigente relacionado con la criptografía.

II. La Entidad Regulada debe recurrir a la autoridad de certificación pública o privada según corresponda para el uso de la Firma Digital.

III. La Entidad Regulada debe implementar certificados de seguridad SSL/TLS para mantener segura las conexiones a Internet, así como para proteger información confidencial que se envía entre los sistemas.

Artículo 49. (Ciclo de vida de desarrollo seguro de software) La Entidad Regulada debe establecer y aplicar procedimientos para el desarrollo seguro de software y sistemas en un ambiente de producción, con el objeto de garantizar que la Seguridad de la Información y Tecnología se diseñe e implemente dentro del ciclo de vida de desarrollo seguro de software y sistemas, considerando lo siguiente:

a. Separación de los entornos de desarrollo, prueba y producción.

b. Establecer estándares de codificación o programación segura.

c. Orientación sobre la seguridad en el ciclo de vida del desarrollo de software.

d. Requisitos de seguridad en la fase de especificación y diseño.

e. Pruebas de las funcionalidades del sistema y seguridad, escaneo de código y pruebas de penetración.

f. Repositorios seguros para el código fuente y la configuración.

g. Seguridad en el control de versiones.

Artículo 50. (Requisitos de seguridad para el desarrollo o adquisición de sistemas) Los requisitos de Seguridad de la Información y Tecnología deben identificarse, especificarse y aprobarse al desarrollar o adquirir sistemas informáticos, con el objeto de garantizar que todos los requisitos de Seguridad de la Información y Tecnología se identifiquen y aborden al desarrollar o adquirir sistemas.

Artículo 51. (Pruebas de seguridad en desarrollo y aceptación) La Entidad Regulada debe definir e implementar, procesos de prueba de seguridad en el ciclo de vida del desarrollo para validar si se cumplen los requisitos de Seguridad de la Información y Tecnología cuando los sistemas informáticos o el código se implementan en el entorno de producción, considerando lo siguiente:

a. Funciones de seguridad autenticación de usuarios, restricción de acceso y uso de criptografía.

b. Codificación segura.

c. Configuraciones seguras incluyendo la de sistemas operativos, firewalls y otros componentes de seguridad.

d. Entradas y salidas esperadas bajo una variedad de condiciones.

e. Criterios para evaluar los resultados.

f. La organización puede aprovechar las herramientas automatizadas, como las herramientas de análisis de código o los escáneres de vulnerabilidades.

Artículo 52. (Desarrollo de sistemas subcontratados) La Entidad Regulada que subcontrata el desarrollo y mantenimiento de sistemas, debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados para garantizar que se implementen medidas de Seguridad de la Información y Tecnología requeridas, considerando lo siguiente:

a. La utilización de software de base aprobado por la Entidad Regulada.

b. Acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el contenido subcontratado.

c. Requisitos contractuales para prácticas seguras de diseño, codificación y prueba.

d. Garantizar que acorde a los sistemas de información, programa o aplicación, el proveedor actualice y entregue la siguiente documentación:

1. Especificación de requerimientos;

2. Diccionario de datos;

3. Diagramas de diseño (Entidad Relación, Flujo de datos, etc.);

4. Manual técnico;

5. Manual de usuario;

6. Documentación que especifique el flujo de la información entre los módulos y los sistemas.

e. Provisión del modelo de amenazas a considerar por desarrolladores externos.

f. Pruebas de aceptación para la calidad y precisión de los entregables.

g. Suministro de evidencia de que se han establecido niveles mínimos aceptables de seguridad y capacidades de privacidad.

h. Derecho contractual a auditar los procesos y controles de desarrollo.

i. La Entidad Regulada debe contar con políticas y procedimientos para la administración de servicios y contratos con terceros, con el propósito de asegurar que los servicios contratados sean provistos en el marco de un adecuado nivel de servicios que minimicen el riesgo relacionado y se enmarquen en las disposiciones contenidas en el presente Reglamento.

Artículo 53. (Separación de los entornos de desarrollo, prueba y producción) La Entidad Regulada debe separar y proteger, los entornos de desarrollo, prueba y producción para proteger el entorno de producción y los datos contra el compromiso de las actividades de desarrollo y prueba, considerando lo siguiente:

a. Separar adecuadamente los sistemas de desarrollo y producción y operarlos en diferentes dominios en entornos físicos o virtuales separados.

b. Definición, documentación e implementación de reglas y autorización para el despliegue de software desde el estado de desarrollo hasta el de producción.

c. Probar cambios en los sistemas y aplicaciones de producción en un entorno de prueba o ensayo antes de aplicarlos a los sistemas de producción.

d. No realizar pruebas en entornos de producción excepto en circunstancias que hayan sido definidas y aprobadas.

e. Mostrar etiquetas de identificación del entorno adecuadas en los menús para reducir el riesgo de error.

f. No se podrá replicar información confidencial o datos personales de los asegurados o beneficiarios en los entornos del sistema de desarrollo y prueba a menos que se proporcionen controles equivalentes al entorno de producción.

Artículo 54. (Gestión de cambios) La Entidad Regulada debe implementar mecanismos y procedimientos para los cambios en las instalaciones de procesamiento de información y sistemas informáticos, con el objeto de preservar la Seguridad de la Información y Tecnología al ejecutar cambios, considerando lo siguiente:

a. Planificación y evaluación del impacto potencial de los cambios considerando todas las dependencias involucradas.

b. Implementar procedimientos y ambientes de prueba, de puesta en producción de versiones nuevas de software.

c. Comunicar los cambios a las partes interesadas pertinentes.

d. Pruebas, aceptación y autorización de cambios.

e. Consideraciones de emergencia y contingencia, incluidos procedimientos de respaldo y de reversión de cambios.

Artículo 55. (Protección de los sistemas informáticos durante pruebas o revisiones de auditoría) En las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de sistemas informáticos, debe planificarse y acordarse entre el evaluador y la Gerencia apropiada, minimizar el impacto de la auditoría y otras actividades de aseguramiento en los sistemas informáticos que afecte las operaciones y servicios.

SECCIÓN V

CONTROLES DE SEGURIDAD FÍSICOS

Artículo 56. (Definición de perímetros físicos de seguridad) La Entidad Regulada debe establecer perímetros de seguridad física con el objeto de proteger las áreas que contienen activos de información previniendo accesos físicos no autorizados y daños o degradación de la información, considerando lo siguiente:

a. Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados con el objeto de asegurar que solo personal autorizado puede acceder físicamente a la entidad.

b. Establecer un área de recepción supervisada por personal u otros medios para controlar el acceso físico a la entidad.

c. Se deben considerar insignias (credencial) fácilmente distinguibles para identificar mejor a los empleados permanentes, proveedores y visitantes.

d. Otorgar acceso restringido al personal del proveedor a áreas seguras o instalaciones de procesamiento de información solo cuando sea necesario, este acceso debe ser autorizado y monitoreado.

e. Restringir el acceso a las áreas de entrega y carga desde el exterior de las instalaciones al personal identificado y autorizado.

Artículo 57. (Asegurar oficinas, ambientes e instalaciones) La Entidad Regulada debe implementar la seguridad física de las oficinas, salas e instalaciones, considerando los siguientes aspectos:

a. Ubicar instalaciones críticas para evitar el acceso del público.

b. Implementar controles para el acceso a los ambientes donde se encuentran los recursos tecnológicos, Gerencia y Archivo de documentación física.

Artículo 58. (Monitoreo de Seguridad Física) La Entidad Regulada debe implementar mecanismos de monitoreo continuo de las instalaciones para detectar accesos físicos no autorizados, considerando los siguientes aspectos:

a. Las instalaciones físicas deben ser monitoreadas por sistemas de vigilancia, que pueden incluir guardias, alarmas contra intrusos, sistemas de monitoreo de video, que puede ser administrado internamente o por un proveedor de servicios de monitoreo.

b. Instalar sistemas de monitoreo de video para monitorear y registrar el acceso a áreas sensibles.

c. El diseño de los sistemas de monitoreo debe mantenerse confidencial, a fin de evitar incidentes no detectados.

d. Establecer los períodos de retención de videos grabados.

Artículo 59. (Protección contra amenazas físicas y ambientales) La Entidad Regulada debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura, considerando lo siguiente:

a. Se debe realizar evaluaciones de riesgos para identificar las posibles consecuencias de las amenazas físicas y ambientales antes de comenzar las operaciones críticas en el sitio físico y a intervalos regulares.

b. Se debe obtener asesoramiento especializado sobre cómo gestionar los riesgos derivados de amenazas físicas y ambientales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, desechos tóxicos, emisiones ambientales y otras formas de desastres naturales o desastres causados por seres humanos.

c. Implementar un plan de evacuación ante emergencias.

Artículo 60. (Trabajo en áreas seguras) La Entidad Regulada debe diseñar e implementar medidas de seguridad para trabajar en áreas seguras, que cubra lo siguiente:

a. Hacer que el personal sea consciente de la existencia de las actividades dentro de un área segura solo en función de la necesidad de comunicarlo.

b. Evitar el trabajo sin supervisión en áreas seguras tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas.

c. Cerrar físicamente e inspeccionar periódicamente áreas seguras.

d. Controlar adecuadamente el transporte y uso de dispositivos de usuario final (equipos de computación) en áreas seguras.

e. Publicar los procedimientos de emergencia de una manera fácilmente visible o accesible.

Artículo 61. (Ubicación y protección de equipos) La Entidad Regulada debe establecer mecanismos para que los equipos de computación se encuentren ubicados en un lugar de manera segura y protegida, según sus capacidades, considerando lo siguiente:

a. Establecer estándares de seguridad en la ubicación de las instalaciones de procesamiento de información que manejan datos confidenciales para reducir el riesgo de que personas no autorizadas tengan acceso a la información durante su uso.

b. Adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales, robo, fuego, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.

c. Monitorear las condiciones ambientales, como la temperatura y la humedad, en busca de condiciones que puedan afectar negativamente el funcionamiento.

d. Aplicar protección contra rayos a todos los edificios y colocar filtros de protección contra rayos en todas las líneas de energía y comunicaciones entrantes.

Artículo 62. (Seguridad de los activos fuera de las instalaciones) La Entidad Regulada debe implementar controles para la seguridad de los activos fuera de las instalaciones, para evitar la pérdida, el daño, el robo o el compromiso de la información almacenada en los equipos de computación y su salida debe estar autorizada, considerando lo siguiente:

a. No dejar equipos y medios de almacenamiento retirados de las instalaciones sin supervisión en lugares públicos y no seguros.

b. Observando las instrucciones del fabricante para proteger el equipo en todo momento.

c. Cuando se transfiere equipo fuera de las instalaciones entre diferentes personas o partes interesadas, se debe mantener un registro que defina la cadena de custodia del equipo que incluya nombres y organizaciones responsables del equipo.

d. Cuando sea necesario y práctico, exigir la autorización para retirar el equipo y los medios de las instalaciones de la organización y mantener un registro de tales retiros para mantener un registro de auditoría.

Artículo 63. (Medios de almacenamiento) La Entidad Regulada debe gestionar los medios de almacenamiento a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación, considerando lo siguiente:

a. Establecer una política específica sobre la gestión de medios de almacenamiento extraíbles y comunicar la misma a cualquier persona que use o manipule medios de almacenamiento extraíbles.

b. Almacenar todos los medios de almacenamiento en un entorno seguro y protegido de acuerdo con su clasificación de información y protegerlos contra amenazas ambientales.

c. Usar técnicas criptográficas para proteger la información en medios de almacenamiento extraíbles para la información confidencial.

d. Solo habilitar puertos de medios de almacenamiento extraíbles si existe una justificación para su uso y la respectiva autorización.

e. Si los medios de almacenamiento que contienen información confidencial deben reutilizarse dentro de la organización, eliminar datos de forma segura o formatear los medios de almacenamiento antes de volver a utilizarlos.

Artículo 64. (Acuerdo de nivel de servicio) I. La Entidad Regulada de forma previa a la contratación de un proveedor externo de tecnología de información debe establecer un acuerdo de nivel de servicio, en el contrato respectivo, que establezca los estándares y la calidad del servicio prestado, de acuerdo con su análisis de riesgo tecnológico y la criticidad de sus operaciones.

II. Los parámetros deben referirse al tipo de servicio, soporte y asistencia a clientes, previsiones para seguridad y datos, garantías del sistema y tiempos de respuesta, disponibilidad del sistema, conectividad, multas por caídas del sistema y/o líneas alternas para el servicio.

Artículo 65. (Seguridad en el cableado) La Entidad Regulada debe proteger los cables que transportan energía, datos o servicios de apoyo contra intercepciones, interferencias o daños, considerando lo siguiente:

a. Las líneas eléctricas y de telecomunicaciones a las instalaciones de procesamiento de información sean subterráneas cuando sea posible, o estén sujetas a una protección alternativa adecuada, como protectores de cables en el piso y postes de servicios públicos.

b. Separar los cables de alimentación eléctrica de los cables de comunicaciones para evitar interferencias.

c. Para sistemas sensibles o críticos, los controles adicionales a considerar incluyen la instalación de conductos blindados y bloqueados, uso de blindaje electromagnético, barridos técnicos periódicos e inspecciones físicas, acceso controlado a paneles de conexión y salas de cables y uso de cables de fibra óptica.

d. Etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.

e. La Entidad Regulada debe contar con la documentación técnica asociada a la infraestructura del cableado debe conservarse actualizada, resguardada y contener como mínimo lo siguiente:

1. Diagrama unifilar eléctrico, donde se muestre las conexiones y componentes principales de los circuitos de la instalación eléctrica.

2. Planos de trayectoria del cableado y ubicación de puntos de salida.

Artículo 66. (Contrato mantenimiento de equipos) La Entidad Regulada podrá tercerizar otros servicios como el mantenimiento de equipos, soporte de sistemas operativos, hospedaje de sitios web, entre otros, para los cuales debe considerar los siguientes aspectos:

a. Tipo de servicio.

b. Soporte y asistencia.

c. Seguridad de datos.

d. Garantía y tiempos de respuesta del servicio.

e. Disponibilidad del servicio.

f. Multas por incumplimiento.

Artículo 67. (Gestión de seguridad en redes y telecomunicaciones) I. La Entidad Regulada debe contar con políticas y procedimientos para la instalación y mantenimiento del hardware y su configuración base, con el propósito de asegurar que proporcionen la plataforma tecnológica que permita soportar las aplicaciones relacionadas con las redes y telecomunicaciones y minimicen la frecuencia e impacto de las fallas de desempeño de las mismas. Para este efecto, se debe establecer un registro formal que contenga toda la información referente a los elementos de configuración del hardware, software, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas de información.

II. La Entidad Regulada debe contar con la documentación técnica asociada a la infraestructura de redes y telecomunicaciones que debe conservarse actualizada, resguardada y contener lo siguiente:

a. Características, topología y diagrama de red.

b. Descripción de los elementos de cableado.

c. Planos de trayectoria del cableado y ubicación de puntos de salida.

d. Diagrama del sistema de interconexión de cables de red, distribución de regletas y salidas.

SECCIÓN VI

OTRAS DISPOSICIONES

Artículo 68. (Sanciones) El incumplimiento a las disposiciones contenidas en el presente reglamento constituyen infracciones sujetas a Procedimiento Administrativo Sancionatorio de conformidad al Reglamento de Sanciones del Sector de Seguros.

Artículo 69. (Responsabilidad) El Gerente General de la Entidad Regulada es responsable de la difusión interna y cumplimiento del presente reglamento.