ASDECITI
Asociación Solidarista de Empleados del Grupo Financiero Citibank de Costa Rica S.A.

REGLAMENTO
GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Junta Directiva de la
ASOCIACIÓN SOLIDARISTA DE
EMPLEADOS DEL GRUPO FINANCIERO
CITIBANK Y AFINES, ASDECITI

15 Julio 2024

Índice

1. Propósito

La seguridad de la información es una disciplina de gestión de riesgos del negocio. La no protección de la información de ASDECITI puede provocar pérdidas financieras y afectar negativamente la marca de ASDECITI. El estándar de seguridad de la información (E.S.I.), establece los requisitos mínimos de seguridad claros y concisos. El estándar de seguridad de la información identifica los requisitos de protección de la información de conformidad con los requisitos jurídicos y reglamentarios pertinentes. De allí que el objetivo de este reglamento es procurar estos estándares representan los requisitos mínimos que ASDECITI deba seguir..

2. Alcance

Las disposiciones establecidas en el presente reglamento son de aplicación obligatoria para todos los miembros de los diferentes órganos de gobierno y administración de la Asociación.

3. Documento de referencia

AD-ES-001 Estatutos de ASDECITI.
AD-RE-004 Reglamento de Ética

4. Definiciones

ASDECITI: Asociación Solidarista de Empleados del Grupo Financiero Citibank y Afines.

Gestión de la tecnología de información: Estructura de relaciones y procesos diseñados y ejecutados para dirigir y controlar la información, sus riesgos asociados y suvinculación con las estrategias y objetivos del negocio.

Proceso: Cadena de actividades que agregan valor y permiten la generación de un producto o servicio bajo determinadas condiciones y plazo.

Perfil tecnológico: Descripción de la estructura organizacional, los procesos y la infraestructura de TI de la entidad, así como del nivel de automatización de sus procesosde negocio y de gestión del riesgo.

Proveedor de tecnologías de información: Persona física o jurídica que provee o prestaun servicio relacionado con la tecnología de información, sea independiente o que pertenezca al mismo grupo o conglomerado financiero, incluyendo las casas matrices.

Riesgo de Seguridad de Información (RSI): Posibilidad de pérdidas financieras derivadas de un evento relacionado con el acceso o uso de la información, que afecta eldesarrollo de los procesos del negocio y la gestión de riesgos de la entidad, al atentar contra la confidencialidad, integridad,

disponibilidad, eficiencia, confiabilidad y oportunidad de la información.

Tecnología de información (TI): Conjunto de técnicas que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizada y utilizada en formaconsistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad.

5. Responsables

La Junta Directiva junto con la Gerencia Administrativa y Financiera serán los responsables de velar por la correcta aplicación de este reglamento.

Los encargados de las unidades ejecutoras deben de cumplir con lo estipulado en este reglamento.

Se debe de realizar la revisión y actualización de este documento por lo menos una vez al año.

6. Reglamento

La Junta Directiva de la ASOCIACIÓN SOLIDARISTA DE EMPLEADOS DEL GRUPO FINANCIERO CITIBANK Y AFINES, ASDECITI, con fundamento en las facultades que le confiere el artículo No. 49 de la Ley de Asociaciones Solidaritas No. 6970, dicta el Reglamento de Ética.

CAPÍTULO PRIMERO: DE LOS OBJETIVOS

ARTÍCULO 1°. - DEL OBJETIVO DE LA ACTIVIDAD REGULADORA DE LA SEGURIDAD DE INFORMACION:

a) Objetivo General: Implementar un esquema de seguridad de la información y ciberseguridad con políticas, estándares y programas de seguridad de la información y Ciberseguridad, de conformidad con lo establecido normativa local aplicable.

b) Objetivos Específicos: Establecer los principios mínimos que la asociación deben implementar para proteger los activos de información y gestionar eficazmente la seguridad de la información en los sistemas informáticos de ASDECITI, de conformidad con los requisitos corporativos, legales y reglamentarios requeridos por la normativa local aplicable.

CAPÍTULO SEGUNDO: DEL COMITÉ DE SEGURIDAD DE LA INFORMACION

ARTÍCULO 2°.- DE LA CONSTITUCIÓN: .El Comité de Seguridad de la información de ASDECITI podrán ser o no Asociados, y en adhesión con el artículo 51 de la Ley 6970 Ley de Asociaciones Solidaritas y con la participación de al menos un miembro de la Junta Directiva de la Asociación en su calidad de coordinador de este comité y considerando que si el Presidente de la Junta Directiva pertenece al comité, no podrá presidirla. Deberá estar conformado por tres miembros. Los Miembros deben contar con experiencia en materia tecnológica, económica, financiera o bancaria. Además, el comité de Información puede contar con la participación de los responsables de las áreas de negocio de la Entidad y con asesores externos a la organización cuando sea necesario para el tratamiento de aspectos técnicos específicos, para que asistan a las sesiones con voz, pero sin voto.

La función principal del Comité de Información es asesorar en temas de tecnología de información y su gestión a la Junta Directiva, sobre la aplicación de políticas para mitigar los riesgos de seguridad de información, el cumplimiento de las regulaciones sobre el particular y la aplicación de los estándares que fueran pertinentes.

ARTÍCULO 3°.- DEL CONFLICTO DE INTERESES: Si al conocer un caso en específico, en el cual se presente un conflicto de intereses con alguno de los miembros del Comité, éste será sustituido por un asociado, escogido por la Junta Directiva. La existencia del conflicto de intereses será determinada por el mismo Comité, absteniéndose de votar el miembro que origine al posible conflicto. Si el miembro cuestionado es el Presidente del Comité, presidirá el mismo la persona que designe el resto de los miembros.

ARTÍCULO 4°.- DE LAS FUNCIONES: Las siguientes son las funciones del Comité:

a) Mantener actualizadas las políticas internas de este reglamento. Asesorar a los responsables en la planificación estratégica de manejo de Información.
b) Desempeñar otras funciones que la Junta Directiva le asigne relacionadas con la gestión de riesgos tecnológicos de información.
c) Recomendar prioridades para las inversiones de Seguridad de Información.
d) Valorar al menos semestralmente o cuando así lo amerite, un reporte sobre el impacto de los riesgos asociados a la Seguridad de Información.
e) Recomendar, asesorar y aprobar el Plan Correctivo-Preventivo derivado de la auditoría y supervisión externa de la gestión de Seguridad de Información.
f) Recomendar y asesorar a la Junta Directiva en cuanto a las políticas generales, lineamientos o directrices de Seguridad de Información, que incluya un esquema de clasificación de información basado en su sensibilidad y criticidad para ASDECITI.
g) Denunciar al comité de ética, el mal manejo de datos, pérdida o manipulación de la información, por el desacato a los protocolos del manejo y seguridad de la información.
h) El comité junto con la administración de ASDECITI deben evaluar periódicamente las siguientes actividades:

a) El cumplimiento del estándar de seguridad de la información y los requisitos técnicos mencionados;
b) El cumplimiento de otras prácticas y procedimientos que la comisión de información, junta directiva o administración pueda exigir cada cierto tiempo.

ARTÍCULO 5°.- DE LAS REUNIONES: La convocatoria de las reuniones del Comité la realizará el Presidente del Comité o al menos por dos de sus miembros. El Comité se reunirá como mínimo una vez al mes, para analizar el cumplimiento de este Reglamento y todas las veces que lo considere necesario.

ARTÍCULO 6°.- DEL QUÓRUM Y LA TOMA DE DECISIONES: El quorum del Comité se conformará con dos de sus miembros. Las decisiones se tomarán por simple mayoría; en caso de empate el voto del Presidente del Comité se computará doble.

CAPÍTULO TERCERO: DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

ARTÍCULO 7.- DE LAS POLÍTICAS REFERENTES A LA SEGURIDAD DE LA INFORMACIÓN:

Las políticas de seguridad de la información deben ser apoyada por otras normas o procedimientos sobre temas específicos que obligan aún más la aplicación de los controles de seguridad de la información y se estructuran normalmente para para cubrir ciertos temas.

A continuación, se detallan aquellas políticas que proporcionan principios y guía en aspectos específicos de la seguridad de la información, los cuales se detallan en los anexos respectivos:

a) Uso aceptable de activos:
   i. Los usuarios son responsables de toda la actividad relacionada con sus IDs de acceso.
   ii. Los usuarios no pueden acceder a cuentas externas de correo electrónico desde la red de ASDECITI para actividades no relacionadas con la Asociación.
   iii. Se prohíbe el uso del acceso remoto a la red global de ASDECITI (por red inalámbrica, banda ancha, por línea conmutada etc.) a menos que la conexión remota utilice una red privada virtual (VPN) aprobada por estándares de dominio tecnológico.
   iv. Los usuarios deben cumplir el Código de ética de ASDECITI.

b) Clasificación de la Información: Protección de Datos, la información confidencial siempre debe estar protegida, ya sea que se esté accediendo, manejando, procesando, almacenando o transmitiendo. Los empleados deberán proteger la información sensible en todas sus formas, incluso la información en forma física que se utilicen o se almacenen en sus espacios de trabajo. Los responsables de la información deben categorizar la información bajo su

control en una de las siguientes clasificaciones de la información y gestionar su control con base a su categoría de riesgo:

i. Restringida.
ii. Confidencial.
iii. Uso Interno
iv. Publica.

c) Gestión de seguridad de red: La red deberán estar protegidas contra amenazas y se deberá mantener la seguridad de los sistemas de información a través de la red.

i. Controles contra malware: Controles de prevención, detección y recuperación para la protección contra los códigos maliciosos (por ejemplo, virus, gusanos, troyanos, programas espías).

CAPÍTULO CUARTO: DE LA CULTURA DE SEGURIDAD DE INFORMACIÓN

ARTÍCULO 10.- DE LA CULTURA DE SEGURIDAD DE LA INFORMACIÓN: El desarrollo del programa de concientización y capacitación y refrescamiento al equipo de ASDECITI, así como la distribución de materiales sobre la seguridad de la información a los empleados. Como mínimo en cuanto a los siguientes temas del estándar de seguridad de la información:

a) Uso aceptable de activos.
b) Clasificación y manejo de la de la Información.
c) Controles de red.

Las Mejores prácticas para los puntos anteriores estos artículos se encuentran en los anexos adjuntos a este reglamento.

CAPÍTULO QUINTO: GESTION DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN

ARTÍCULO 11.- RESPONSABILIDADES Y PROCEDIMIENTOS: La administración deberá garantizar se aplique un enfoque eficaz a la gestión de los incidentes de seguridad de la información y cumpla el estándar del proceso del equipo de respuesta a incidentes de seguridad, que en su respectivo caso sería la Gerente General de la Asociación:

a) Cuando un evento de seguridad satisfaga la definición de incidente de seguridad, hay que generar un incidente de seguridad de la información.
b) La administración deberá definir procesos para responder a un incidente de seguridad de conformidad con el proceso de Gestión. Esto incluye, sin limitaciones, alertas generados por sistemas de detección de intrusos, sistemas de prevención de intrusos, detección de anomalías en el comportamiento de la red.

ARTÍCULO 12.- REPORTES Y DENUNCIAS DE DEBILIDADES DE SEGURIDAD DE LA

INFORMACIÓN: Todos los incidentes de seguridad deberán reportarse de conformidad con el estándar del proceso del equipo de respuesta a incidentes de seguridad, que en su caso el equipo de respuesta estaría conformado por la Gerente General de la Asociación, y el coordinador del Comité de Seguridad de la información, que evaluaran el caso y harán las escalaciones respectivas según lo ameritan a la Junta Directa o al proveedor de sistemas.

a) Se deberán tomar medidas inmediatas contra cualquier actividad sospechosa.
b) Todos los empleados, contratistas y proveedores externos deben denunciar todos los incidentes de seguridad, reales o posibles.
c) El equipo de respuesta a incidentes de seguridad deberá mantener un proceso de contención de incidentes de seguridad de la información que afecten a la asociación. Incluye, sin limitaciones, la monitorización de las actividades de los intrusos, la búsqueda y el aislamiento de los sistemas comprometidos, la eliminación de los medios de acceso de los intrusos y la comunicación a grupos internos y externos en la medida de lo necesario.
d) El equipo de respuesta a incidentes de seguridad deberá mantener un proceso que:
    - Se ponga en contacto con los empleados y los equipos adecuados para cerciorarse que los sistemas, programas y datos se restaurarán;
    - Garantice que se cuenta con la experiencia adecuada que estarán disponible para las labores de contención, erradicación y recuperación en todos los eventos, incluso incidentes de ciberseguridad a gran escala.

CAPÍTULO SEXTO: DE LAS DISPOSICIONES FINALES

ARTÍCULO 13.- DEL CONOCIMIENTO DEL REGLAMENTO: Las personas asociadas, miembros de la Junta Directiva, y demás comités deben conocer el presente Reglamento, por lo que no podrán argumentar desconocimiento de algún criterio o disposición establecida en él.

ARTÍCULO 14.- DE LA COMUNICACIÓN DE LAS REFORMAS DEL REGLAMENTO: Una vez que se aprueben las modificaciones al Reglamento de Inversiones, la Junta Directiva tiene que comunicarlas a las personas asociadas, en un plazo no mayor de 15 (quince) días hábiles.

ARTÍCULO 15.- DE LOS CASOS NO PREVISTOS POR EL REGLAMENTO: Los casos no previstos en este Reglamento los resolverá la Junta Directiva, siempre y cuando no pugnen con las disposiciones legales y estatuarias de la Asociación.

ARTÍCULO 16.- DE LA REVISIÓN MÍNIMA DEL REGLAMENTO: Es obligación de la Junta Directiva hacer, como mínimo, una revisión anual de este Reglamento; en dicha revisión tienen que participar al menos los integrantes de la Junta Directiva, del Comité de Seguridad de Información y el Gerente

General de la Asociación. La revisión valorara si hay cambios regulatorios, tendencias tecnológicas, condiciones económicas, o cualquier otra razón.

Aprobado en sesión del 12 de octubre de 2020. Rige a partir de la fecha de su publicación.

TRANSITORIOS

TRANSITORIO UNO: Este reglamento rige a partir del comunicado oficial que la Junta Directiva realice a los afiliados de la Asociación, por los medios suficientes para que éstos tengan acceso al mismo.

TRANSITORIO DOS: Este Reglamento deroga todas las disposiciones anteriores, salvo aquellas que sean más beneficiosas para el asociado..

Control de cambios	Fecha y Acta
Aprobación del Reglamento de Gestión de seguridad de la Información	12 octubre 2020 - ACTA Nº.108-JD. P2019/2020

ANEXO UNO: USO ACEPTABLE DE ACTIVOS

Introducción

Los equipos, sistemas y servicios de ASDECITI, que incluyen: computadoras, teléfonos, correo de voz, computadoras portátiles, facsímil (servicios de fax), intranet, acceso a Internet, correo electrónico, mensajes de texto (SMS), instantáneo la mensajería y otras herramientas de comunicación electrónica, dispositivos, enlaces de datos y servicios de datos para uso in situ, móvil o remoto se proporcionan para permitirle realizar las tareas relacionadas con su trabajo.

Todos los empleados deben usar dichos dispositivos, equipos y servicios de acuerdo con el Código de Conducta y las Políticas y mejores prácticas de ASDECITI.

Objetivo General: Proveer guía y recomendaciones sobre el uso y cuidado de las laptops de ASDECITI de acuerdo al ARTÍCULO 9 y 10 de este reglamento.

Requerimientos mínimos:

1. Bloquear la Computadora cada vez que se deja la estación de trabajo.
2. Mantener la computadora con candado en cada momento, utilizar siempre el cable de seguridad, sea en la oficina, ferias, charlas, y otros eventos donde se lleve la laptop.
3. Mantener la computadora bajo llave cuando están fuera de la oficina. Ejemplo en vacaciones.

4. En caso de robo de la laptop deben avisarle a la administración inmediatamente, la cual debe proveerle al colaborador el número de serie de la laptop robada. Seguidamente deben irse para la oficina del OIJ a interponer la denuncia para registrar el robo. Esto es requerido por dos motivos: Primero para efectos de si aparece la laptop que se pueda identificar y segundo se requiere para efectos de cobro del seguro contra robo. La administración debe contar con el registro del número de serie de cada laptop, tenerlo a mano para que se lo pueda brindar a la persona en el momento requerido y se pueda registrar en la denuncia del OIJ).

5. Totalmente prohibido compartir las claves ya que esto es catalogado como “Phishing” que significa Suplantación de identidad.

6. No instale aplicaciones que no están relacionadas al uso exclusivo de ASDECITI.

7. No conectar una laptop de la Asociación a los puertos de red de CITI ya que estas laptops no tienen la configuración de políticas de seguridad de CITI. Esto causa que en el momento en que se conecte una laptop de estas con el cable de red a un puerto en un cubículo de CITI causa que el puerto de red reconozca que no es una laptop de CITI y bloquea el puerto de red y emite una alerta a los equipos de CTI.

Recomendaciones adicionales:

1. Planifique su viaje de regreso a casa si tiene que llevar la computadora portátil con usted. Si debe asistir al supermercado, la universidad, el restaurante o la casa de familiares y/o amigos, lleve la computadora con usted. En caso de que no vayan para su casa, sino que van para otros lugares procuren no llevarse la laptop que lo exponga a un asalto o perdida de la misma.

2. No olvide poner la atención de donde está la computadora. Si va a un lugar público inseguro se recomienda dejar la computadora en la oficina bajo cerradura o con candado en el escritorio.

3. Mantenga su computadora portátil segura en su camino a casa, esto incluye guardarla dentro de la bolsa de la computadora portátil, no dejarla desatendida en ninguna de sus paradas, tampoco utilizarla mientras se está en tránsito.

4. Asegúrese de que el espacio del hogar donde deja la computadora sea seguro, no la deje en el garaje, o cerca de ventanas que puedan ser violentadas.

5. Si eres víctima de robo, no te expongas, coopera y no te resistas.

6. Cuando finalice la jornada laboral apague y desconecte de la electricidad para alagar la vida útil de las baterías.

7. No deje su computadora en el automóvil, ni siquiera en la cajuela, ya que hoy en día es muy fácil detectar una computadora con un escáner especial que identifica dispositivos electrónicos en el

automóvil. No hay un estacionamiento seguro. Lleve la computadora con usted lo más que pueda. No lo pierdas de vista.

ANEXO DOS CLASIFICACIÓN DE LA INFORMACIÓN

Introducción

El manejo de se refiere a la clasificación de información de acuerdo con su nivel de riesgo asociado y cómo manejar posteriormente esa información. Clasificar (y reclasificar) la información es la parte más importante del manejo de la información y ayuda a determinar cómo se transmite, almacena y desecha esa información.

Objetivo General: Proveer guía y recomendaciones para la gestión de riesgo en la protección de datos e información de ASDECITI de acuerdo al ARTÍCULO 9 y 10 de este reglamento.

Manejo de Información: El manejo de la información hace referencia a cuatro actividades:

1. Clasificación de la información y, según dicha clasificación
2. Transmisión.
3. Almacenamiento.
4. Eliminación.

Clasificación de Información: La clasificación determina el modo de transmitir, almacenar y eliminar la información.

Si la información que está clasificando puede utilizarse sola o en combinación para identificar a una persona directa o indirectamente, se trata de “información personal identificable” (PII) y se debe asignar el atributo PII.

Para gestionar este tipo información la administración y el comité gestionaran un inventario de control de archivos para monitorear que los documentos (archivo, reporte, informe, etc) que la

asociación maneja, cumplan con los controles de seguridad de información en su transmisión, almacenaje y desecho, de acuerdo al tipo de clasificación asignada, de acuerdo a la sensibilidad de los datos que maneja.

A modo de resumen, en el siguiente cuadro, se muestran el tipo de información, así como los requisitos mínimos de manejo y control de la información que se deben cumplir:

<table>
<tr><th>Clasificación de la información</th><th>Transmisión</th><th>Almacenamiento</th><th>Eliminación</th></tr>
<tr><td>PII restringida</td><td rowspan="2">Cifrar en transmisiones internas y externas.</td><td rowspan="2">Cifrar en todos los entornos.</td><td rowspan="4">Desechar en contenedor de desecho aprobado por Citi en una ubicación de Citi.</td></tr>
<tr><td>Restringida</td></tr>
<tr><td>PII confidencial</td><td rowspan="2">Cifrar en transmisiones externas.</td><td rowspan="2">Cifrar cuando se almacena fuera de la infraestructura administrada por Citi.</td></tr>
<tr><td>Confidencial</td></tr>
<tr><td>PII interna</td><td rowspan="4">No requiere manejo especial.</td><td rowspan="4">No requiere manejo especial.</td><td>No requiere manejo especial, pero se recomienda desechar en un contenedor aprobado en una ubicación de Citi.</td></tr>
<tr><td>Interna</td><td rowspan="3">No requiere manejo especial.</td></tr>
<tr><td>PII pública</td></tr>
<tr><td>Pública</td></tr>
</table>

Requisitos protección de Información sensible:

1. Escritorios y pantallas limpios: Los empleados deberán proteger la información sensible en todas sus formas, incluso la información en forma física que se utilicen o se almacenen en sus espacios de trabajo. Los negocios deberán comunicar este requisito a todos los empleados por lo menos una vez al año a través de las labores de concientización sobre la seguridad de la información.

2. Siempre debe trabajar en documentos de utilizando únicamente herramientas y equipo remoto aprobadas por la empresa. Nunca deben enviarse a un dispositivo externo.

3. Está prohibido reenviar el correo electrónico de la empresa que contenga los siguientes tipos de información: Independientemente de si el correo electrónico está cifrado o no. El material que no debe enviarse por correo electrónico a una dirección de correo electrónico personal incluye:

   a. Información Confidencial.

   b. Información de identificación personal (PII) que no pertenece al remitente,

   c. Información clasificada solo como uso interno.

4. Las excepciones al reenvío de correos electrónicos internos a una dirección de correo electrónico personal:

    a. Se permite enviarse documentos relacionados con su propia información personal, incluidos recibos de pago y documentos fiscales utilizando solo el correo electrónico seguro.

    b. Cualquier documentación también se puede enviar por correo electrónico a correos electrónicos personales utilizando solo el correo electrónico seguro y específicamente acordado por la Gerencia y marcado de acuerdo con esta frase específica: " No hay restricciones para reenviar esto a una dirección personal de correo electrónico para imprimir en casa ".

Requisitos de Cifrado de Información sensible:

1. Los datos confidenciales, PII confidenciales y restringidos deben cifrarse cuando se almacena en cualquier entorno electrónico, servidor en la nube, sharedrive, etc. O en caso que sea un documento físico almacenar en gabinete bajo llave.

2. Los datos confidenciales, PII confidenciales y restringidos deben cifrarse cuando se envían por correo electrónico fuera de la red de ASDECITI.

3. Los archivos cifrados SecureZIP pueden adjuntarse a un correo electrónico regular enviado a destinatarios internos o externos o pueden almacenarse en archivos compartidos o sitios de SharePoint en la red.

4. Se puede hacer el Cifrado mediante una frase de contraseña: este método se utiliza para cifrar archivos que se enviarán a destinatarios externos o a destinatarios internos.

    a. Para cifrar el archivo, ingrese una frase de contraseña, que el destinatario deberá abrir y ver el archivo en texto sin formato.

        i. Cree el archivo encriptado usando SecureZIP: En la pantalla de cifrado en SecureZIP, ingrese una frase de contraseña.

        ii. Envíe el archivo SecureZIP encriptado al destinatario como archivo adjunto a un correo electrónico normal.

        iii. Proporcione al destinatario la frase de contraseña que se configuró al crear el archivo cifrado SecureZIP. Esto debe ser hecho "fuera de banda", por teléfono o por otro método que el correo mismo electrónico.

iv. Descifrar el archivo: el destinatario debe ingresar la frase de contraseña para abrir y ver el archivo.

Requisitos de desecho/eliminación de información:

1. Para los controles del desecho de archivos se establece el siguiente protocolo:
    a. Solicitar el inventario de documentos a revisar, para identificar:
        i. Fecha de bodegaje.
        ii. Levantar lista de documentos o cajas a desechar.
    b. Elaborar el acta de desecho de la papelería que cumple con una antigüedad de al menos 6 años.
    c. Firma del acta por parte del coordinador del comité de Seguridad de la Información y del Gerente General de ASDECITI.
    d. Enviar el correo a la empresa Access con el dato de la persona que de parte de ASDECITI, realizará la visita con la lista autorizada a desechar.
    e. Elaborar un certificado de que la papelería que cumpla con el plazo de almacenaje fue debidamente desechada, indicar nombre de la persona que realizó el proceso, junto con el encargado de ASDECITI, al final del proceso de desecho ambos deben firmar probando de esta forma que se cumplió con el desecho de papelería autorizada.

ANEXO TRES: GESTIÓN DE SEGURIDAD DE RED

Introducción

Las redes deberán estar protegidas contra amenazas y se deberá mantener la seguridad de los sistemas de información a través de la red. Esto incluye información transmitida por la red.

Objetivo General: Proveer guía y recomendaciones para la gestión de la seguridad de la red de datos de la asociación de acuerdo al ARTÍCULO 9 y 10 de este reglamento.

Requisitos mínimos de control de Seguridad de Red:

1. La administración deberá cerciorarse que todas las aplicaciones y todos los servicios de Internet de la Asociación que estén alojados en sitios de terceros cuentan con servicios contra ciberataque o ataque informático aprobados por estándares de dominio tecnológico.
2. Sólo se podrán utilizar sistemas de seguridad de la red y proveedores de servicios de seguridad aprobados por estándares de dominio tecnológico o controles validados por un proceso de

evaluación de seguridad de la información de terceros (por ejemplo, cortafuegos, sistemas de detección/prevención de intrusos, etc.)

a. Para lo anterior se debe hacer revisión anual de licencias y validar su renovación con base al inventario de Licencias que la asociación cuenta de sus programas y plataformas con los proveedores externos.

b. Revisión anual de los Certificación de cumplimientos que los proveedores de sistemas externos mantengan en materia de privacidad de la información, políticas de manejo de información confidencial y datos personales, control de acceso a la infraestructura y sistemas tecnológicos, políticas de mantenimiento de sistemas y manejo de vulnerabilidades. Dentro de las que se pude validar:

   i. Certificación “Tier” del centro de datos, lo que garantiza que las instalaciones están diseñadas y construidas para satisfacer las necesidades y continuidad del negocio.

   ii. Certificación de Servicios en la nube, como el Microsoft 365 (MS365) y Azure, como herramienta para monitorear y medir la efectividad de su Sistema de Gestión de Continuidad Comercial (BCMS por sus siglas en Ingles).

7. Control de Cambios

Versión: 1	**Articulo Actual**	**Artículo Modificado**
Revisado por: Comité de Crédito		
Aprobado por: Junta Directiva		
Número de acta: xxxx-000-2024		
Fecha de aprobación: 22/7/2024		