PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDIA MUNICIPAL DE SAN BERNARDO DEL VIENTO

2020-2021

COMPROMETIDOS CONTIGO

INTRODUCCIÓN

El presente plan se elabora con el fin de dar a conocer como se realizara la implementación y socialización del componente de Gobierno en línea en el Eje temática de la Estrategia en Seguridad y privacidad de la información, el cual busca guardar los datos de los ciudadanos como un bien estratégico, garantizando la seguridad de la información.

El proceso de administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a la Alcaldía Municipal de Suesca minimizar perdidas de información y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento e sus funciones, están sometidos a riesgos que pueden hacer fracasar su gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos.

1. OBJETIVOS

1.1 Objetivo General

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la Alcaldía de San Bernardo del Viento, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

1.2 Objetivo Específicos

- Concientizar a todos los funcionarios, contratistas y terceros en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.
- Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en la Alcaldía Municipal de San Bernardo del Viento para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

2. METODOLOGIA

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información la Alcaldía Municipal de San Bernardo del Viento, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. Diagnosticar

2. Planear

3. Hacer

4. Verificar

5. Actuar

Ilustración 1 – Marco de Seguridad y Privacidad de la Información

Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

3. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acceso a la Información Pública** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.
- **Archivo** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al

- servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenazas** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Bases de Datos Personales** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Ciberseguridad** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales

debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- **Declaración de aplicabilidad** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada** Es aquella información que estando en poder o

custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Plan de tratamiento de riesgos** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Riesgo** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

4. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- Alta Dirección: aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.
- Proceso Administración del Sistema Integrado de Gestión: Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.
- Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los

procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

- Servidores públicos y contratistas: ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.
- Quien haga las veces de Control Interno: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

5. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Alcaldía Municipal de San Bernardo del Viento, adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

1. Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.

2. Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

3. Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.

4. Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.

5. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

6. Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.

7. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Alta Dirección de la administración municipal asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, el presente plan forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar la materialización del riesgo.

6. EVALUACIÓN DEL RIESGO

Para realizar un análisis de los riegos, se procede a identificar los objetos que deben ser protegidos, los daños que pueden sufrir, sus posibles fuentes de daño y oportunidad, su impacto en la compañía, y su importancia dentro del mecanismo de funcionamiento. Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, y en último término, en caso de ocurrencia de estos, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

6.1 Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

a) Personal
b) Hardware
c) Software y utilitarios
d) Datos e información
e) Documentación
f) Suministro de energía eléctrica
g) Suministro de telecomunicaciones

6.2 Daños

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.
b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, llámese por ejemplo, cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

6.3 Prioridades

La estimación de los daños en los bienes y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los Servicios que se pierden en el acontecimiento. Por lo tanto, los bienes de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

6.4 Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal del La biblioteca asociadas al Centro de operaciones Computacionales son:

Acceso no autorizado

Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones). Ruptura de las claves de acceso a los sistemas computacionales.

a) Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).
b) Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

Desastres Naturales

a) Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de soporte (edificios) y/o de operación (equipos computacionales). b) Inundaciones causados por falla en los suministros de agua.

c) Fallas en los equipos de soporte:

- ✓ Por fallas de la red de energía eléctrica pública por diferentes razones ajenas.
- ✓ Por fallas de la comunicación.
- ✓ Por fallas en el tendido físico de la red local.
- ✓ Fallas en las telecomunicaciones con instalaciones externas.
- ✓ Fallas de Personal Clave – Se considera personal clave aquel que cumple una función vital en el flujo de procesamiento de datos u operación de los Sistemas de Información:
  a) Personal de Informática (Ingeniero, pasantes a cargo del soporte).
  b) Personal de la Administración Municipal.

Pudiendo existir los siguientes inconvenientes:

a) Enfermedad.

b) Accidentes.

c) Renuncias.

d) Abandono de sus puestos de trabajo.

Fallas de Hardware

a) Falla en el Servidor de Aplicaciones y Datos, tanto en su(s) disco(s) duro(s) como en el procesador central.

b) Falla en el hardware de Red:

- Falla en los Switches.
- Falla en el cableado de la Red.

c) Falla en el Router.

6.5 Expectativa Anual de Daños

Para las pérdidas de información, se deben tomar las medidas precautorias necesarias para que el tiempo de recuperación y puesta en marcha sea menor o igual al necesario para la reposición del equipamiento que lo soporta.

7. MEDIDAS PREVENTIVAS

7.1 Control de Accesos

Se debe definir medidas efectivas para controlar los diferentes accesos a los activos computacionales:

a) Acceso físico de personas no autorizadas.

b) Acceso a la Red de PC's y Servidor.

c) Acceso restringido a las librerías, programas, y datos.

d) Acceso restringido a través de cuentas de usuario administrador.

7.2 Previsión de desastres Naturales

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en los equipos de la alcaldía municipal de San Bernardo del Viento, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico u otro fenómeno natural pueda generar mediante su caída y/o destrucción, la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, el tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, discos con información vital de respaldo de aquellos que se encuentren aun en las instalaciones.

7.2.1 Adecuado Soporte de Utilitarios

Las fallas de los equipos de procesamiento de información pueden minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, nos referimos a:

a) UPS de respaldo de actual servidor de Red o de estaciones críticas
b) UPS de respaldo switches y/o HUB's

7.2.2 Seguridad Física del Personal

Se deberá tomar las medidas para recomendar, incentivar y lograr que el personal comparta sus conocimientos con sus colegas dentro de cada área, en lo referente a la utilización de software y elementos de soporte relevantes. Estas acciones permitirán mejorar los niveles de seguridad, permitiendo los reemplazos en caso de desastres, emergencias o períodos de ausencia ya sea por vacaciones o enfermedades.

7.2.3 Seguridad de la Información

La información y programas de los Sistemas de Información que se encuentran en el Servidor, o de otras estaciones de trabajo (portátiles o equipos computo) críticas deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado (creación Back up).

8. PLAN DE RESPALDO

El Plan de Respaldo trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento.

8.1 Respaldo de datos Vitales

Se deberá identificar las áreas para realizar respaldos:

a) Sistemas en Red.

b) Sistemas no conectados a Red.

c) Sitio WEB.

8.2 Objetivos del Plan de Recuperación

Los objetivos del plan de Recuperación son:

1) Determinación de las políticas y procedimientos para respaldar las aplicaciones y datos.

2) Planificar la reactivación dentro de las 12 horas de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.

3) Permanente mantenimiento y supervisión de los sistemas y aplicaciones. 4) Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.

8.2.1 Alcance del Plan de Recuperación

El objetivo es restablecer en el menor tiempo posible el nivel de operación normal del centro de procesamiento de la información, basándose en los planes de emergencia y de respaldo a los niveles del Centro de Cómputos y de los demás niveles. La responsabilidad sobre el Plan de Recuperación es de la Administración, la cual debe considerar la combinación del personal, equipos, datos, sistemas, comunicaciones y suministros.

1. Todos los miembros de las áreas de recuperación deben estar informados y entrenados, así como poseer una copia del Plan de Contingencia.

2. Una copia del plan debería mantenerse almacenado Biblioteca Pública, junto con los respaldos.

9. SOLUCIÓN PROPUESTA Y PLAN DE CONTINGENCIAS

De acuerdo al análisis de riesgos y a la revisión de seguridad realizada, se presentan las sugerencias de los casos para combatir cada uno de los riesgos potenciales a los que se enfrenta la red informática.

9.1 Recomendaciones Contra La Acción De Virus

La situación actual en la sección de esquema de antivirus, es necesario estandarizar el software de antivirus en todas las estaciones de trabajo y servidores. Es aconsejable tener un proveedor de software antivirus para las estaciones y otro diferente para el servidor, para reducir la probabilidad de que un virus que no esté en la lista de actualización, se filtre en toda la red.

9.2 Recomendaciones Contra Accesos No Autorizados

Frente a este riesgo potencial, es necesario implementar lo siguiente:

9.2.1 Recomendaciones A Nivel Físico

- ✓ El servidor de archivos no debe ser accesible físicamente a cualquier persona
- ✓ Es conveniente que exista un espacio físico donde se ubique el servidor, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su funcionamiento, como temperatura ambiental adecuada, aislado del polvo y plagas dañinas.
- ✓ En este espacio, además de ubicar el servidor, se pueden ubicar los elementos más sensibles de la red corporativa como el HUB/Switch y el servidor proxy**.**

9.3 Recomendaciones Para Prevenir Fallas En Los Equipos

Se deberá realiza periódicamente una vez por semana una revisión general (hardware y software) de los equipos de cómputo pertenecientes a la entidad. Otra opción es contratar los servicios de personal apto para que realice de forma mantenimiento preventivo a los equipos y correctivo si lo amerita la situación (esto en caso de no poseer personal apto internamente ingeniero de Sistemas). Sea la decisión que se que se escoja se sugiere que como mínimo se realice por lo menos una vez al mes y llevar un control, de la vida útil de los diferentes dispositivos.

10. ACTIVIDADES PREVIAS AL DESASTRE

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, las cuales nos asegurarán un proceso de Recuperación con el menor costo posible. Establecimiento de plan de acción En esta fase de planeamiento se debe de establecer los procedimientos y normas a seguir relativos a:

a) Instalaciones físicas. En caso de que se pueda suscitar un robo, sismo o incendio se deberían tomar las siguientes medidas preventivas:

Robos

- ✓ Al entrar y salir de las instalaciones se deberá observar previamente de que no exista ningún individuo sospechoso.
- ✓ Queda prohibido dar información personal de los empleados o información confidencial de la organización.
- ✓ Contar con personal para resguardo de las instalaciones de la empresa.
- ✓ Instalación de alarma.
- ✓ Contratar con pólizas de seguros

Sismos:

- ✓ Ubicar y revisar periódicamente, que se encuentren en buen estado las instalaciones de AGUA, y SISTEMA ELECTRICO.
- ✓ Fijar a la pared repisas, cuadros armarios, estantes, espejos y libreros. Evitar colocar objetos pesados en la parte superior de éstos, además asegurar al techo las lámparas.
- ✓ Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín, de ser posible un radio portátil y una linterna con pilas.
- ✓ Todo el personal debería portar siempre una identificación.
- ✓ Realizar simulacros de manera periódica.

Incendios:

- ✓ Estar siempre alerta. La mejor manera de evitar ios incendios, es la prevención.
- ✓ Procurar no almacenar productos inflamables.
- ✓ Cuidar que los cables de los aparatos eléctricos se encuentren en perfectas condiciones.
- ✓ No se deben realizar demasiadas conexiones en contactos múltiples, para evitar la sobre carga de los circuitos eléctricos.
- ✓ Por ningún motivo mojar las instalaciones eléctricas. Recuerde que el agua es un buen conductor de la electricidad.
- ✓ Todo contacto o interruptor debe tener siempre su tapa debidamente aislada.
- ✓ Aparatos eléctricos estén apagados o perfectamente desconectados.
- ✓ Que prohibido fumar en las instalaciones debido a que este habito contaminante, no deja una buena impresión y puede causar desagrado ante los no fumadores o puede causar un incendio.
- ✓ Bajo ningún motivo se debe sustituir los fusibles por alambre o monedas, ni usar cordones eléctricos dañados o parchados.
- ✓ Contar con una alarma de incendios.
- ✓ Tener en un lugar visible y accesible un extintor contra incendios.
- ✓ Realizar simulacros de manera periódica.

- ✓ Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín.

b) Equipos de cómputo Inventario actualizado de los equipos de manejo de información (computadoras, impresoras, etc), especificando su contenido (software que usa) y su ubicación.
c) Obtención y almacenamiento de los respaldos de información (BACKUPS)

11. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La alcaldía municipal de San Bernardo del Viento, evaluará el ejercicio de "tratamiento de riesgos y privacidad de la información", por medio de seguimientos para revisar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario. De esta forma conlleva, dado el caso, a evidenciar todas aquellas situaciones que pueden estar influyendo en la aplicación de las acciones de tratamiento.