	periódicas por el sector donde se encuentra ubicadas las instalaciones

No se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización del Jefe de Cada Área y el coordinador de Sistemas, esto demuestra que los equipos se encuentran protegidos por cada funcionario autorizado. Tampoco se han reportado casos donde haya habido hurtos de nuestro sistema computo en la fundación sin embargo se recomienda siempre estar alerta.

3.4.3. Falla en los equipos

Situación Actual	Acción correctiva
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.
La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de quipos que están para dar de baja.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Colocar estabilizadores a todos los equipos de la Fundación universitaria Navarra -UNINAVARRA

Analizando el riesgo de falla de los equipos, es recomendable estar realizando mantenimiento preventivo a los equipos computo e implementar estabilizadores a los equipos para en caso de una falla de energía eléctrica los dispositivos se puedan apagar correctamente.

3.4.4. Acción de virus informático

Situación Actual	Acción correctiva
Se cuenta con un software antivirus para la entidad, pero su actualización no se realiza de forma inmediata a su expiración.	Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del nuevo antivirus.

Situación Actual	Acción correctiva
Únicamente el área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad.	Se cumple
Los antivirus no se actualizan periódicamente en cada equipo.	El área de Tic's instalara y revisara periódicamente que los antivirus de los equipos sigan con la licencia, de lo contrario la tienen que renovar.

Tener actualizado e instalado los antivirus para todos los equipos computo de la Fundación Universitaria Navarra- UNINAVARRA para prevenir daños por causa de un virus informático.

3.4.5. Terremoto

- **Sin Pérdida O Daños Menores De Las Instalaciones:** El siniestro puede afectar únicamente parte de la estructura de las instalaciones, en cuyo caso no se verían afectados los datos, sin embargo, podría ser necesario evacuar las instalaciones trasladando al personal fuera de las instalaciones, el impacto provocaría en la Gobernación sería menor, puesto que las actividades se interrumpirían por unas horas o hasta por un día completo.
- **Con Pérdida De Las Instalaciones:** La pérdida de las instalaciones afectaría gravemente a las operaciones de la Gobernación del Meta y los datos pueden verse dañados seriamente. En esta parte de la contingencia es donde se requiere que todas las medidas de emergencia y de recuperación funcionen adecuada y oportunamente.

3.4.6. Sabotaje

La protección contra el sabotaje requiere:

- Una selección rigurosa de los colaboradores.
- Buena administración de los recursos humanos.
- Buenos controles administrativos.
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.

Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

El problema de la seguridad del computador debe ser tratado como un problema importante de dirección. Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Se menciona a continuación algunas medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles:

- Ubicar los equipos en lugares más seguros en donde se prevea cualquier contingencia de este tipo.
- Mantener una lista de números telefónicos de las diferentes dependencias policiales a mano y en lugares donde se pueda hacer un llamado de emergencia.
- Siempre habrá de tomarse en cuenta las Políticas de Seguridad en caso como terrorismo y sabotaje. Es importante la medida de ingreso de personas debidamente identificadas, marcación de zonas de acceso restringido, prevención para explosivo, etc.
- Mantener adecuados archivos de reserva (backup)
- Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Montar procedimientos para remitir registro de almacenamiento de archivos y recuperarlos.
- Usar rastros de auditoría o registro cronológico (Logs) de transacción como medida de seguridad.

4. PLAN DE RECUPERACION Y RESPALDO DE LA INFORMACION

4.1. Actividades previas al desastre

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. Se establece los procedimientos relativos a: Sistemas e Información, Equipos de Cómputo, Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

- **Sistemas de Información:** La Entidad cuenta con una relación de los Sistemas de Información de software de datos, para respaldarla con backup.
- **Equipos de Cómputo:** Se debe tener en cuenta el catastro de Hardware, impresoras, scanner, módems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación o buscar información importante.
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la entidad.

4.2. Falla en las comunicaciones (Teléfono, internet)

Ante una falla en las comunicaciones (telefonía fija e internet), se optará por la telefonía móvil, para lo cual se informará el número celular de emergencia a las entidades aseguradoras que con mayor frecuencia tenemos contacto, esta línea la tendría a cargo el recepcionista y los líderes de los procesos.

Para soportar una falla en las comunicaciones, la clínica realizara las siguientes actividades:

• Contar con un celular con minutos permanente en registro y control.

• Entrenar al recepcionista para que pueda brindar la información adecuada ante estos casos.

CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
2016-SEP-14	01	Documento inicial.

ELABORÓ		REVISÓ		APROBÓ	
Nombre	Shirly Marcela Ardila	**Nombre**	Jhonatan Díaz	**Nombre**	Camilo Lozano
Cargo	Coordinadora de Calidad	**Cargo**	Auxiliar de Tic's	**Cargo**	Representante por la Dirección