EQUIPO DE CÓMPUTO.

Realizar un diagnóstico de su equipo de cómputo ya que el constante uso de la computadora genera múltiples errores como fallas de carga del sistema, virus informáticos, programas mal instalados, configuraciones mal realizadas, actualizaciones no instaladas etc., que si bien la computadora está diseñada para realizar pequeñas reparaciones de software, constantemente realiza omisiones de pasos para continuar con las operaciones más complicadas y poder mantener estable el sistema, pero estas pequeñas fallas, se acumulan y en gran cantidad pueden generar un problema mayúsculo

<table>
<tr><th colspan="3">EQUIPO DE CÓMPUTO.</th></tr>
<tr><th>Nivel de Impacto: MEDIA</th><th>Probabilidad de Severidad o Gravedad: OCASIONAL</th><th>Grado de Riesgo o Rango: MODERADA</th></tr>
<tr><td colspan="3">ANTES Plan de Respaldo:
En caso de fallas a nivel hardware:
1. Realizar mantenimientos preventivos para evitar, reducir y, cuando aplique, reparar las fallas, evitar accidentes sobres los bienes y equipo de seguridad de la empresa.
2. Respaldo diario de información de cada una de las computadoras en el servidor de respaldo de archivos (http:10.20.30.5/nextcloud)
3. Evitar accesos no autorizados de personal a áreas sensibles (ingreso no autorizado a las instalaciones, lugares restringidos al personal SITE o tomar archivos restringidos).
4. Respaldo de correos electrónicos diario, mismo que se realiza de forma automática ya que los correos electrónicos son administrados por la empresa Google.

En caso de fallas a nivel software:
1. Realizar diagnóstico lógico de las PC (memoria ram, disco duro, procesador, energía, etc).
2. Contar con licencias originales de la paquetería básica para la operatividad de la PC (Office y Windows).
3. Realizar mantenimiento preventivo para evitar, reducir y, cuando aplique, reparar las fallas.</td></tr>
<tr><td colspan="3">ANTES Plan de Respaldo:
En caso de Vandalismo
1. Verificar intento de vandalismo ya sea menor o mayor, podría afectar a las PCs, periféricos y servidores, así como las comunicaciones.
2. Establecer vigilancia mediante cámaras de seguridad en el sitio, el cual registre todos los movimientos de entrada del personal.
3. Determinar lugares especiales, fuera del centro de datos, para almacenarlos medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación.
4. Contar con contrato o mediante convenio, con un centro de cómputo alterno de características físicas y equipo de cómputo adecuado para darle continuidad a las operaciones críticas de la empresa, aún en forma limitada de cobertura y de comunicaciones.</td></tr>
<tr><td colspan="3">ANTES Plan de Respaldo:
En caso de Huelga
1. Determinar lugares especiales, fuera del centro de datos, para almacenarlos respaldos y copia de la documentación de referencia.
Departamento de Sistemas y Soporte Técnico debe de dar la alerta del paro total y sacar los respaldos de información fuera del edificio dentro de un tiempo límite antes de ser declarada la huelga.
Departamento de Sistemas y Soporte Tecnico debe prever un sitio alterno para continuar con las operaciones críticas.</td></tr>
</table>

EQUIPO DE CÓMPUTO.		
Nivel de Impacto: MEDIA	**Probabilidad de Severidad o Gravedad: OCASIONAL**	**Grado de Riesgo o Rango: MODERADA**

DURANTE Plan de Emergencia:

En caso de fallas a nivel Hardware y Software.

1. Detectar la instalación de software de comportamiento errático y/o dañino para la operación de los sistemas informáticos en uso (virus, sabotaje, hackers).
2. Si las fallas se derivan del mal funcionamiento de un equipo (Hardware) se procede a su reemplazo inmediato o remitirse al mantenimiento.
3. Instalar (sí lo amerita) el sistema operativo.
4. Restaurar la información de las bases de datos y programas.
5. Revisar y probar la integridad de los datos.
6. Corrección de las alteraciones que se localicen en los servidores Hardware.
7. Corrección de las alteraciones que se localicen en los servidores Software.
8. Revisión y prueba de la integridad de los datos.
9. Restaurar las configuraciones personalizadas de todo el software secundario para la operatividad de la PC
10. Iniciar las operaciones

DURANTE Plan de Emergencia:

En caso de Vandalismo

1. En caso de intento de vandalismo se deberá reportar a las instancias correspondientes para dar atención a los problemas presentados.
2. Verificar si existen usuarios que realicen intromisión no autorizada a procesos y/o datos de los sistemas, ya sea por simple curiosidad o malas intenciones.

DURANTE Plan de Emergencia:

En caso de Huelga

1. Se tendrá que establecer un tiempo límite de espera de solución de la huelga como por ejemplo 24 horas con el fin de que no afecte el servicio proporcionado a las demás áreas o al cliente, si después de este intervalo la huelga continuara, se determinará el lugar o lugares de reubicación alternos.
2. Recoger los respaldos de datos, programas, manuales y claves del lugar en el que se encuentren resguardados.

DESPUÉS Plan de Recuperación:

En caso de fallas a nivel Hardware y Software.

1. Detectar si los problemas ocasionados fueron por movimientos sísmicos, huracanes, tornados, ciclones inundaciones, que afecten directa o indirectamente a las instalaciones físicas de soporte (edificios).
2. Identificar posibles fallas en los equipos de soporte que pudieran ser originadas por:
   - ✓ Problemas de Energía eléctrica pública.
   - ✓ Problemas en las Comunicaciones Problemas de Red local.
   - ✓ Problemas en las Telecomunicaciones.
   - ✓ Problemas de Telefonía.
   - ✓ Problemas de Internet**.**
   - ✓ Problemas lógicos del hardware.
   - ✓ Problemas de configuraciones.

Estos casos se pueden llegar a presentar por diferentes razones ajenas al manejo por parte de la empresa.
Llevar a cabo un inventario de equipo de cómputo, software y mobiliario, para determinar cuál es la información crítica que se tiene que resguardar, adicionalmente levantar un inventario de los servicios de cómputo, telecomunicaciones, Internet, etc., que son requeridos para que los usuarios estén en posibilidad de llevar a cabo sus actividades normales.
Identificar los tipos de siniestros a los cuales está propenso cada uno de los procesos críticos, tales como falla eléctrica prolongada, incendio, terremoto, etc.

DESPUÉS Plan de Emergencia:

En caso de Vandalismo

1. Identificar intento de vandalismo ya sea menor o mayor, podría afectar a las PCs, periféricos y servidores, así como las comunicaciones
2. En caso de que se violen las claves de acceso a los sistemas informáticos deberá verificar grabaciones de CCTV para llamar a los involucrados y dar atención a los problemas derivados del incumplimiento.
3. Aplicar las sanciones necesarias dependiendo de la gravedad del incidente y en caso de ser necesario levantar acta administrativa y/o la rescisión del contrato.

EQUIPO DE CÓMPUTO.		
Nivel de Impacto: MEDIA	**Probabilidad de Severidad o Gravedad: OCASIONAL**	**Grado de Riesgo o Rango: MODERADA**
4. Reasignar claves de acceso a correos, usuarios, servidores, etc.		
DESPUÉS Plan de Recuperación: **En caso de Huelga** 1. Identificar el conjunto de amenazas que pudieran afectar a los procesos informáticos, ya sea por causa accidental o intencional. 2. Se debe estar preparado para cualquier percance, verificando que dentro de la empresa se cuente con los elementos necesarios para salvaguardar sus activos. 3. Se deben analizar las funciones de mayor prioridad de la empresa, por medio de diagramas de flujo de los procesos específicos para medir el alcance de cada actividad.		