Procedimiento de Auditoría del Equipo Informático de Trabajo

1. Objetivo

Establecer un procedimiento detallado para que el equipo de IT realice auditorías en los equipos informáticos de los empleados, garantizando la seguridad, el cumplimiento normativo y la protección de datos. El procedimiento aplica tanto a auditorías remotas como presenciales.

2. Alcance

Este procedimiento se aplica a todos los empleados que utilicen equipos informáticos de la empresa, ya sean portátiles, estaciones de trabajo o dispositivos de acceso remoto.

3. Responsabilidades

- **Equipo de IT:** Realizar la auditoría siguiendo los pasos definidos, documentar hallazgos y tomar medidas correctivas si es necesario. Revisar y actualizar periódicamente este procedimiento para garantizar su efectividad.
- **Empleado:** Permitir el acceso al equipo, colaborar en el proceso y reportar cualquier incidente de seguridad.

4. Procedimiento de Auditoría

4.1. Preparación (Antes de la Auditoría)

1. **Notificación al Empleado:** Enviar una comunicación formal indicando la fecha, hora y alcance de la auditoría.
2. **Recolección de Información:**
    a. Confirmar el sistema operativo y software instalado.
    b. Identificar accesos a redes internas o recursos sensibles.
    c. Revisar logs de actividad si están disponibles.

3. **Definir el Modo de Auditoría:**
    a. **Remota:** Utilizar herramientas de acceso remoto seguras (ej. AnyDesk, TeamViewer, Microsoft Intune, VPN segura).
    b. **Presencial:** Coordinar un punto de encuentro en la oficina o sitio de trabajo.
4. **Herramientas Necesarias:**
    a. Software de monitoreo y escaneo (Ej: antivirus corporativo, escaneo de vulnerabilidades...).
    b. Listado de comprobación (checklist) para evaluar el equipo.

4.2. Ejecución de la Auditoría (Durante la Revisión)

1. **Verificación de Seguridad:**
    a. Estado y actualización del sistema operativo y software crítico.
    b. Presencia y configuración del antivirus/cortafuegos.
    c. Revisión de conexiones remotas activas y accesos no autorizados.
    d. Revisión de configuraciones de acceso a datos corporativos y herramientas de cifrado.
2. **Validación de Políticas de Seguridad:**
    a. Uso de contraseñas seguras y autenticación multifactor (MFA).
    b. Revisión de permisos de usuario y configuraciones de acceso.
    c. Verificación de almacenamiento de datos sensibles (uso de dispositivos USB, nube, etc.).
3. **Detección de Anomalías:**
    a. Revisión de logs del sistema y actividad sospechosa.
    b. Presencia de software no autorizado o malware.
    c. Conexiones sospechosas en la red interna o acceso a servidores.

4.3. Finalización y Reporte (Después de la Auditoría)

1. **Registro de Hallazgos:** Documentar cualquier vulnerabilidad, software desactualizado o configuraciones incorrectas.
2. **Medidas Correctivas:**
    a. Si se detectan riesgos de seguridad, implementar correcciones inmediatas.
    b. Reforzar las políticas de seguridad en caso de incumplimiento.
3. **Entrega del Informe:**
    a. Compartir un informe con el empleado y su responsable, detallando los hallazgos y recomendaciones.
    b. Escalar problemas críticos de seguridad y cumplimiento.
4. **Seguimiento:**
    a. Realizar auditorías periódicas según lo establecido por la política de la empresa.
    b. Asegurar la implementación de mejoras y controles de seguridad.

5. Buenas Prácticas

- **Protección de Datos:** Toda la información recolectada en la auditoría debe tratarse con confidencialidad.
- **Cumplimiento Normativo:** Seguir las regulaciones de protección de datos y seguridad de la información aplicables (GDPR, ISO 27001, etc.).
- **Uso Ético de Herramientas de Auditoría:** No recopilar ni manipular información personal fuera del alcance definido.

6. Auditoría y Revisión del Procedimiento

El presente procedimiento será revisado periódicamente para garantizar su vigencia y adaptabilidad a nuevas amenazas y requisitos corporativos.