

11. Formación y Concienciación

Actividad:

- Elaboración de un **cronograma de capacitación anual** que incluya sesiones semestrales.
- Ejemplo: Capacitación “Reconociendo amenazas digitales: phishing y ransomware”.
- **Simulaciones de phishing** trimestrales con una meta del 80-90% de éxito en detección.
- Redacción y difusión de **guías de buenas prácticas** en el uso de contraseñas y navegación segura.

Propósito:

Incrementar la conciencia de los empleados para evitar vulnerabilidades humanas y asegurar que sean la primera línea de defensa frente a amenazas.

12. Gestión de Proveedores

Actividad:

- Incluir **cláusulas de seguridad** en todos los contratos con proveedores (ej. obligación de cifrar datos sensibles).
- Realizar **auditorías periódicas** para revisar el cumplimiento de estas cláusulas.

Propósito:

Garantizar que todos los proveedores cumplan con los estándares mínimos de seguridad requeridos por la organización.

13. Auditorías y Revisión

Actividad:

- Programar **auditorías internas semestrales**.
- Verificar configuraciones críticas como **firewalls** y **logs de accesos**.
- Evaluar políticas implementadas para identificar oportunidades de mejora.

Propósito:

Evaluar periódicamente la efectividad de la Política de Seguridad de la Información (PSI) para realizar ajustes y mejoras continuas.

14. Consecuencias del Incumplimiento

Actividad:

- Definir un **sistema de sanciones** escalonado:
 - Primera infracción: **Advertencia escrita.**
 - Segunda infracción: **Suspensión temporal.**
 - Infracciones graves o reiteradas: **Terminación del contrato laboral.**

Propósito:

Garantizar el cumplimiento de la PSI mediante medidas disciplinarias claras y conocidas por todo el personal.

15. Referencias

Actividad:

- Incluir una sección de referencias que contemple:
 - **Normas internacionales** como **ISO/IEC 27001** (gestión de seguridad).
 - **Legislación nacional/local**, por ejemplo, la **Ley de Protección de Datos Personales.**

Propósito:

Alinear la PSI con estándares reconocidos y normativas legales vigentes para asegurar su validez y aplicabilidad.