Alejandro Molina

13/10/2025

Informe de Seguridad – DataProtect S.L

Tabla de contenido

1. Parte – Comprensión teórica

1.1. Política de seguridad

Una política de seguridad es un conjunto de normas y procedimientos que ayudan a proteger los sistemas, datos y recursos de una organización. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información, evitando problemas como pérdidas de datos o accesos no autorizados.

1.2. Herramientas para análisis y gestión de riesgos

- **Análisis FODA:** Identifica fortalezas, debilidades, oportunidades y amenazas, y ayuda a planificar cómo minimizar riesgos.
- **ISO 27005 / OCTAVE / CRAMM:** Evalúan riesgos sobre activos de información y ayudan a definir medidas de seguridad.

1.3. Diferencia entre auditoría total y parcial

- **Auditoría total:** Revisa todos los sistemas, procesos y activos de la organización.
- **Auditoría parcial:** Analiza únicamente un área concreta, como un servidor, base de datos o departamento específico.

1.4. Plan de contingencias

Procedimientos para que la empresa continúe funcionando ante incidentes o fallos. Subplanes principales:

- **Respaldo:** Copias de seguridad de datos importantes.
- **Emergencia:** Medidas inmediatas para proteger personas y sistemas.
- **Recuperación:** Acciones para restaurar servicios y datos a su estado normal.

1.5. Modelo de seguridad – RBAC

En un centro educativo:

- **Profesor:** Acceso solo a sus clases y calificaciones.
- **Alumno:** Solo a sus notas y materiales de estudio.
- **Administrativo:** Acceso a registros administrativos.
  Así, cada usuario accede únicamente a lo que necesita.

2. Parte – Caso práctico: caída del servidor

2.1. Informe de política de seguridad

Para evitar incidentes como la caída del servidor principal, se recomienda: monitoreo constante, copias de seguridad automáticas, control de accesos, mantenimiento preventivo y protocolos claros para la gestión de incidentes. Además, capacitar al personal en buenas prácticas de seguridad.

2.2. Auditoría parcial

- **Activos a revisar:** Servidores, bases de datos, sistemas de respaldo y red interna.
- **Herramientas:** Nmap (análisis de red), Nessus (vulnerabilidades) y revisión de logs.

2.3. Plan de contingencias básico

- **Respaldo:** Copias automáticas diarias, almacenadas en servidor secundario y nube.
- **Emergencia:** Apagado seguro, notificación al equipo de TI y comunicación a empleados y clientes.
- **Recuperación:** Restauración de datos desde la última copia, verificación de integridad y reinicio progresivo.

2.4. Modelo de seguridad – RBAC

Roles definidos:

- **Administrador:** Acceso total a sistemas.
- **Técnico de soporte:** Acceso solo a mantenimiento.
- **Administrativo:** Solo a los datos que necesita.
  Esto protege la información sensible.

3. Parte – Esquema visual

POLÍTICA DE SEGURIDAD

v

AUDITORÍA

v

PLAN DE CONTINGENCIAS <-> MODELOS DE SEGURIDAD

- Iconos sugeridos: escudo (política), lupa (auditoría), carpeta con respaldo (contingencias), llave o candado (modelos de seguridad).

4. Listados y tablas

Activo	Riesgo / Vulnerabilidad	Medida preventiva / correctiva / recuperación
Servidor principal	Caídas, fallos de hardware	Monitoreo, mantenimiento preventivo, backup
Base de datos clientes	Pérdida de información	Copias automáticas, cifrado
Red interna	Accesos no autorizados	Firewall, control de accesos, RBAC
Equipo administrativo	Malware o errores humanos	Antivirus, capacitación, backups

Estas medidas aseguran que los datos estén protegidos, los sistemas funcionen correctamente y se eviten accesos no autorizados, garantizando la continuidad del negocio.

5. Conclusión final

Los principales riesgos en DataProtect S.L. son: caída de servidores, pérdida de datos y accesos no autorizados. Aplicando políticas de seguridad, auditorías periódicas y un plan de contingencias sólido, la empresa puede minimizar estos riesgos y mantener la información protegida, asegurando la continuidad de sus operaciones.