Actividad Evaluable (E3)

1. Describa de forma sencilla el sistema informático y detalle los requerimientos de seguridad física
2. Elabore un formulario y planifique entrevista con el personal que considere necesario, para la realización de un Análisis de Gestión de Riesgo

DESCRIPCIÓN GENERAL DE LA PRÁCTICA:

Esta actividad evaluable consiste en:

Una organización dedicada a servicios de consultoría necesita implantar un Centro de Proceso de Datos (CPD) externo para alojar sus sistemas de información. Los departamentos y el número de trabajadores son:

- Administración (5)
- Comercial (5)
- Recursos Humanos (3)
- Operaciones (20)
- Informática (2)

Se debe diseñar un sistema informático adecuado y considerar los requisitos de seguridad física y lógica necesarios para proteger el CPD.

1. Describa de forma sencilla el sistema informático (Servidores, red, almacenamiento, seguridad…) y detalle los requerimientos de seguridad física (ubicación, control de acceso, protección contra incendios, condiciones ambientales, redundancia, disponibilidad…) y lógica (Autenticación y autorización, monitoreo y auditoría, Protección de datos, Actualización y parches, seguridad de red…) que tendría en cuenta:
    a. Sistema informático (Servidores, red, almacenamiento, seguridad…)
    b. Requerimientos de seguridad física (ubicación, control de acceso, protección contra incendios, condiciones ambientales, redundancia, disponibilidad…)
    c. Requerimientos de seguridad lógica (Autenticación y autorización, monitoreo y auditoría, Protección de datos, Actualización y parches, seguridad de red…).

2. Elabore un formulario y planifique entrevista con el personal que considere necesario, para la realización de un Análisis de Gestión de Riesgo.

1. Describa de forma sencilla el sistema informático y detalle los requerimientos de seguridad física

La Organización que se dedica a servicios de consultoría necesita implementar un Centro de Proceso de Datos (CPD), con un sistema informático robusto y que supere los requisitos de seguridad física y lógica. Sus aspectos más fundamentales son:

SISTEMA INFORMÁTICO:

1. **Servidores:**
    a. **Tipo**: Servidores blade o rack para así optimizar el espacio y gestión.
    b. **Cantidad**: Al menos 4 servidores de alta disponibilidad para cubrir los servicios críticos y asegurarse la redundancia:
        i. **Servidor 1**: Aplicaciones de Negocio (ERP, CRM).
        ii. **Servidor 2**: Bases de Datos.
        iii. **Servidor 3**: Servidores Web.
        iv. **Servidor 4**: Servidores para Copias de Seguridad y Recuperación.

2. **Red**:
    a. **Switches**: Switches gestionados de alta capacidad para la segmentación de las redes (VLANs).
    b. **Routers**: Routers redundantes para asegurar la conectividad constante.
    c. **Firewall**: Firewalls de nueva generación (NGFW) para la protección avanzada contra las amenazas.
    d. **VPN**: VPNs para el acceso remoto seguro de los empleados.

3. **Almacenamiento**:
    a. **SAN/NAS**: Sistemas de almacenamiento en red (SAN o NAS) para el almacenamiento centralizado y acceso rápido.
    b. **Capacidad**: Capacidad para al menos 10 TB inicialmente, con expandir dicha capacidad.
    c. **RAID**: Configuraciones RAID (RAID 5 o 6) para la tolerancia a los fallos.

4. **Seguridad**:
    a. **Antivirus/Antimalware**: Soluciones robustas de antivirus y antimalware.
    b. **IDS/IPS**: Sistemas de detección y prevención de intrusiones.
    c. **Backup**: Sistema de copias de seguridad automatizadas y plan de recuperación ante distintos desastres (humanos y/o naturales).

REQUERIMIENTOS DE SEGURIDAD FÍSICA:

1. **Ubicación**
    a. **Accesibilidad**: Ubicación geográfica segura, lejos de las áreas propensas a desastres naturales.
    b. **Proveedor**: Selección de un proveedor de CPD con instalaciones certificadas (ISO 27001).

2. **Control de Acceso**:
    a. **Autenticación**: Uso de las tarjetas de acceso, biometría y control de acceso basado en roles.
    b. **Registro**: Registro y monitoreo de las entradas y salidas del personal.

3. **Protección contra Incendios**:
    a. **Sistemas**: Instalación de sistemas de detección y extinción de incendios (detectores de humo, rociadores, sistema de gas inerte).
    b. **Procedimientos**: Planes de evacuación y respuestas a las emergencias.

4. **Condiciones Ambientales**:

   a. **Climatización**: Sistemas HVAC (calefacción, ventilación y aire acondicionado) redundantes para mantener la temperatura y humedad controlados.
   b. **Monitoreo**: Sensores y sistemas de monitoreo ambiental para detectar cambios críticos.

5. **Redundancia y Disponibilidad**:
   a. **Energía**: UPS y generadores de energía de respaldo.
   b. **Conectividad**: Conexiones a Internet redundantes a través de los diferentes proveedores.
   c. **Disaster Recovery**: Plan de recuperación antes desastres (DRP), que estén probados y actualizados en ese momento.

REQUERIMIENTOS DE SEGURIDAD LÓGICA:

1. **Autenticación y Autorización**:
   a. **MFA**: Autenticación multifactor (MFA) para el acceso a sistemas críticos.
   b. **Roles**: Implementación de controles de acceso basados en roles (RBAC).

2. **Monitoreo y Auditoría**:
   a. **Logs**: Registro de logs de acceso y actividades.
   b. **SIEM**: Sistemas de gestión de información y eventos de seguridad (SIEM) para los análisis y correlación de eventos.

3. **Protección de Datos**:
   a. **Cifrado**: Cifrado de datos en tránsito (TLS/SSL) y en reposo.
   b. **Políticas**: Políticas de retención y destrucción segura de los datos.

4. **Actualización y Parches**:
   a. **Parches**: Programa de gestión de parches para mantener todos los sistemas actualizados.
   b. **Escaneo**: Escaneos regulares de vulnerabilidades.

5. **Seguridad de Red**:
   a. **Segmentación**: Segmentación de redes y VLANs para aislar y proteger los diferentes tipos de tráfico.

b. **DDoS**: Protección contra ataques de denegación de servicio (DDoS).
c. **VPN**: VPNs seguras para el acceso remoto.

2. Elabore un formulario y planifique entrevista con el personal que considere necesario, para la realización de un Análisis de Gestión de Riesgo

FORMULARIO:

Si se quiere realizar un formulario para un personal, es fundamental recopilar la información necesaria, precisa y detallada a través de entrevistas con el personal clave de la organización:

1. **Información General del Entrevistado**:
    - Nombre:
    - Departamento:
    - Cargo:
    - Años en la Empresa:
    - Contacto:

2. **Identificación de Activos**:
    - Sistemas:
    - Datos:
    - Infraestructura:
    - Personal:

3. **Evaluación de Amenazas**:
    - **¿Qué tipos de amenazas considera que pueden afectar a los activos críticos?**
        - Amenazas naturales (incendios, inundaciones, terremotos)
        - Amenazas humanas (hacking, sabotaje, errores humanos)
        - Amenazas tecnológicas (fallos de hardware/software)
        - Amenazas externas (competencia, robos, espionaje)

4. **Evaluación de Vulnerabilidades**:
    - **¿Qué vulnerabilidades existen actualmente en los sistemas y procesos?**
        - Fallos de seguridad
        - Procedimientos obsoletos
        - Capacitación del personal
        - Dependencia de proveedores externos

5. **Impacto de las Amenazas**:
    - **¿Cuál sería el impacto en su departamento si se materializan las amenazas identificadas?**
        - Pérdida de datos
        - Interrupción de servicios
        - Daño a la reputación
        - Pérdida financiera

6. **Medidas de Mitigación**:
    - **¿Qué medidas están implementadas para mitigar las amenazas y vulnerabilidades identificadas?**
        - Políticas y procedimientos de seguridad
        - Tecnologías de protección
        - Capacitación del personal
        - Planes de contingencia

7. **Necesidades y Recomendaciones**:
    - **¿Qué necesidades adicionales de seguridad considera que deberían abordarse?**
    - **¿Tiene alguna recomendación específica para mejorar la gestión de riesgos en su departamento?**

8. **Comentarios Adicionales**:
    - **¿Desea agregar algún comentario adicional sobre la gestión de riesgos?**

PLANIFICACIÓN DE LA ENTREVISTA:

El objetivo de la entrevista es que se realice un Análisis de Gestión de Riesgo detallado para identificar y mitigar amenazas y vulnerabilidades que puedan afectar a la implementación y operación del CPD externo.

1. **Participantes Clave**:
    a. **Director de TI**: El objetivo es obtener la visión general de la infraestructura tecnológica y políticas de seguridad actuales.
    b. **Gerente de Operaciones**: El objetivo es comprender los procesos críticos y sus dependencias tecnológicas.
    c. **Jefe de Administración**: El objetivo es identificar los riesgos financieros y de gestión relacionados con el CPD.
    d. **Gerente de Recursos Humanos**: El objetivo es evaluar la capacitación del personal y políticas de seguridad.
    e. **Responsable de Seguridad**: El objetivo es analizar las medidas de seguridad físicas y lógicas implementadas.
    f. **Representante del Departamento Comercial**: El objetivo es identificar los riesgos relacionados con la pérdida de datos de clientes y comunicaciones.

2. **Agenda de la Entrevista**:
    a. Presentación del Proyecto (15 minutos):
        - Introducción y objetivos del Análisis de Gestión de Riesgo.
        - Explicación del proceso y metodología.
    b. Entrevista con el Director de TI (45 minutos):
        - Discusión sobre la infraestructura actual, políticas de seguridad y planes de contingencia.
    c. Entrevista con el Gerente de Operaciones (45 minutos):
        - Evaluación de procesos críticos, dependencias tecnológicas y posibles interrupciones.
    d. Entrevista con el Jefe de Administración (45 minutos):
        - Análisis de riesgos financieros y de gestión asociados con el CPD.
    e. Entrevista con el Gerente de Recursos Humanos (45 minutos):
        - Evaluación de la capacitación del personal y políticas de seguridad.
    f. Entrevista con el Responsable de Seguridad (45 minutos):
        - Análisis de las medidas de seguridad física y lógica implementadas.
    g. Entrevista con el Representante del Departamento Comercial (45 minutos):
        - Identificación de riesgos relacionados con datos de clientes y comunicaciones.

3. **Conclusión y Próximos Pasos (15 minutos)**:
    a. Resumen de hallazgos preliminares.
    b. Planificación de los siguientes pasos y cronograma de las acciones.
4. **Notas Adicionales**:
    a. Las entrevistas pueden ser realizadas en persona o virtualmente, según la disponibilidad del personal.
    b. Se recomienda grabar las entrevistas (con el consentimiento de los participantes) para asegurar que no se pierda ninguna información importante.
    c. Distribuir el formulario de entrevista con antelación para que los entrevistados puedan preparar sus respuestas.