Parte 1 – Identificación de medidas de seguridad

A partir del contexto de la empresa, identifica y explica brevemente:

1. Dos medidas de seguridad aplicadas al edificio (no informáticas).

   Las dos medidas aplicadas al edificio son:

   Sistema de entrada y salida con tarjetas/contraseñas: lo que protege son los datos de la empresa que se puedan llevar físicamente, actúa sobre el problema de robos, seria especialmente útil en situaciones las cuales hay mucha gente trabajando físicamente y no se puede tener un control absoluto sobre quién entra y quien sale.

   Sistema de alarma y cámaras de vigilancia: lo que protege son las zonas en las cuales hay mucha información confidencial, actúa sobre el problema de robos intrusiones, seria especialmente útil cuando no haya nadie en las oficinas y en horario no laboral como los fines de semana.

2. Dos medidas de seguridad aplicadas a los sistemas informáticos.

   Dos medidas de seguridad aplicadas a los sistemas son:

   Antivirus: Protege el ordenador de posibles ataques, actúa frente Malware, ransomware y ataques externos, y es útil en situaciones cuando se usa mucho internet y para las descargas

   Autenticación con usuario y contraseña: Protege a la información privada de la empresa y de la persona, actúa sobre suplantación de identidad y accesos no autorizados

3. Una medida pensada para prevenir incidentes.

SAI: protege a los dispositivos sobre los picos de corriente y/o la interrupción de esta actúa sobre problemas de sobre tensión de corriente o apagón, es útil en situaciones donde en un determinado corto tiempo no hay acceso a corriente

4. Una medida pensada para reducir el impacto cuando el incidente ya ha ocurrido.

   Copias de seguridad recurrentes: protege la información y los datos de la empresa actúa sobre la perdida de datos y sea por fallos de hardware, errores humanos o ataques es útil en situación en las que se han borrado datos por error o te los han robado.

Parte 2 – Análisis de información y datos

La empresa gestiona diferentes tipos de información.

2.1 Clasificación de la información

Indica si la siguiente información es sensible, crítica o de bajo impacto, y justifica brevemente:

Información	Impacto	Justificación
Lista de correos de clientes	Sensible	Ya que son datos personales de clientes
Horarios de los empleados	Bajo	Ya que no lleva ninguna información critica
Código de fuente interno	Critico	Ya que es la base de la empresa
Catalogo publico de servicios	Bajo	Ya que la información es publica
Copias de contratos firmados	Critico	Ya que pueden suponer una suplantación de identidad
Fotografías de eventos corporativos	Bajo	Ya que no supone nada negativo a la empresa

2.2 Riesgos asociados

Elige tres de los elementos anteriores y explica:

- **Lista de correos de clientes:** Lo que pasaría si se perdieran los correos es que afectaría a la hora de poder comunicarse con sus clientes y perder el contacto. Si fueran modificados podrían ponerse correos con links con malware y problemas a la hora de comunicarse con los clientes y si la lista se hiciera pública la empresa podría tener sanciones económicas, problemas legales con los clientes y mala reputación para la empresa
- **Código de fuente interno:** Lo que pasaría si se perdieran los códigos, sería la paralización completa del desarrollo de software, si se modificara lo que pasaría seria que podría poner muchos errores y podrían hacer vulnerable la seguridad de la empresa, y si se hicieran públicos lo que pasaría seria que las empresas rivales podrían copiarlo y/o mejorarlo para superarlos.
- **Copias de contratos firmados:** Lo que pasaría seria que podrían tener problemas legales, si se modificaran los contratos podría haber cambios de no autorizados hacia las condiciones de los trabajadores, y si los contratos se hicieran públicos lo que pasaría seria que tendrían problemas legales ya que se ha expuesto información confidencial de todos los trabajadores.

Parte 3 – Almacenamiento y disponibilidad

DataNova quiere mejorar la disponibilidad de su información.

3.1 Elección de soluciones

Para cada situación, elige la opción más adecuada y justifica:

a) Archivos que se usan constantemente durante la jornada laboral: **Servidor Local**
b) Información histórica que casi nunca se consulta: **Almacenamiento en la nube**
c) Datos que no se pueden perder bajo ningún concepto**. Servidor local + almacenamiento en la nube.**

3.2 Estrategia de continuidad

Explica cómo garantizarías que la empresa pueda seguir trabajando si:

- El servidor local deja de funcionar: Garantizaría poder seguir trabajando, tendiendo las copias en la nube
- La oficina queda inaccesible durante varios días: Teletrabajo con un sistema remoto de autentificación
- Un error humano borra información importante: Recuperar la información gracias a las copias de seguridad

Parte 4 – Incidente de seguridad

Un empleado descarga un archivo desde una web aparentemente legítima. Horas después, varios equipos empiezan a comportarse de forma extraña y algunos archivos dejan de abrirse. El servidor principal sigue funcionando, pero la empresa decide desconectarlo por precaución.

Responde:

1. Qué tipo de incidente podría estar ocurriendo.

   El tipo de incidente que estaría ocurriendo sería un ataque de malware o ransomware

2. Qué acciones inmediatas debería tomar la empresa.

   Desconectar los equipos infectados, informar sobre el ataque

3. Qué información es prioritaria proteger en ese momento.

   La información prioritaria son las copias de seguridad, los usuarios y contraseñas, el código fuente y los datos tanto de los trabajadores como de los clientes.

4. Qué medidas podrían haberse aplicado para reducir el impacto.

   Las medidas que se podrían haber aplicado serian un buen antivirus, permisos para poder instalar, y una buena formación sobre seguridad

5. Qué cambios harías para evitar que vuelva a suceder.

   Los cambios que haría serian, implementación de permisos para que no todo el mundo pudiera descargar cosas de internet y un buen curso de seguridad

Parte 5 – Diseño de una solución global

Los datos principales se almacenarían en un servidor local conjunto con un sistema de copias de seguridad cifradas en la nube, el acceso serio mediante uso de usuarios y contraseñas robustos como también con el sistema Authenticator, las copias de seguridad se harán automáticamente cada día, el sistema se revisaría cada 5/6 meses, y el responsable de la seguridad sería un administrador, aparte de hacer un curso sobre la importancia de la seguridad cada 4 meses.