Ejercicio 2 UD1. SAD. PRINCIPIOS DE LA SEGURIDAD INFORMATICA

Analiza y comenta a que principios de la seguridad informática van relacionados los siguientes supuestos. Los 5 primeros están resueltos.

1. Acceso no autorizado a datos sensibles: Un empleado intenta acceder a información confidencial de clientes sin tener los permisos adecuados.
Principios aplicables: Confidencialidad.

2. Phishing en correos electrónicos: Un usuario recibe un correo que parece ser de su banco, solicitando que ingrese su información personal.
Principios aplicables: Autenticación.

3. Uso de contraseñas débiles: Un grupo de empleados utiliza la misma contraseña para múltiples cuentas.
Principios aplicables: Integridad y autenticación.

4. Fugas de datos por dispositivos perdidos: Un empleado pierde su laptop que contiene información sensible de la empresa.
Principios aplicables: Confidencialidad.

5. Actualizaciones de software ignoradas: Un sistema operativo no se actualiza regularmente, lo que lo hace vulnerable a ataques.
Principios aplicables: Integridad, disponibilidad

6. Redes Wi-Fi inseguras: Un empleado se conecta a una red Wi-Fi pública para trabajar, sin usar una VPN.

7. Malware en dispositivos: Un usuario descarga un archivo de una fuente no confiable y su dispositivo se infecta con malware.

8. Falta de copias de seguridad: Una empresa no realiza copias de seguridad de sus datos críticos y sufre un ataque de ransomware.

9. Ingeniería social: Un atacante se hace pasar por un técnico de soporte para obtener información confidencial de un empleado.

10. Acceso físico no controlado: Personas no autorizadas pueden acceder a las instalaciones de la empresa sin supervisión.

Determina de los siguientes supuestos cuales eson relativos al No Repudio en origen o en destino.

1. Firma Digital en Contratos: Un usuario firma digitalmente un contrato electrónico. Posteriormente, el usuario intenta negar que haya firmado el contrato. La firma digital proporciona evidencia de que el usuario es el autor del documento.

2. Correo Electrónico Autenticado: Un empleado envía un correo electrónico a su supervisor con información confidencial. Si el empleado intenta negar haber enviado el correo, el registro del servidor de correo y la firma digital del mensaje pueden demostrar su autoría.

3. Transacciones Financieras: Un cliente realiza una transferencia bancaria en línea. Si el cliente intenta negar que realizó la transacción, el banco puede presentar registros de la firma digital y la autenticación del cliente.

4. Acceso a Sistemas: Un usuario accede a un sistema crítico utilizando credenciales únicas. Si el usuario intenta negar haber accedido al sistema, los registros de auditoría y la autenticación de dos factores pueden servir como prueba.

5. Acuse de Recibo de Mensajes: Un empleado envía un mensaje importante a su equipo y solicita un acuse de recibo. Si el destinatario intenta negar haber recibido el mensaje, el acuse de recibo sirve como prueba de que lo recibió.

6. Confirmación de Entrega de Paquetes: Un servicio de mensajería envía un paquete y proporciona un comprobante de entrega al destinatario. Si el destinatario intenta negar que recibió el paquete, el comprobante sirve como evidencia.

7. Registro de Acceso a Aplicaciones: Un usuario accede a una aplicación y recibe una notificación de que su acceso ha sido registrado. Si el usuario intenta negar que utilizó la aplicación, el registro de acceso puede demostrar lo contrario.

8. Notificaciones de Cambios en Políticas: Una empresa envía una notificación a todos los empleados sobre un cambio en las políticas de seguridad. Si un empleado intenta negar haber recibido la notificación,