

FORMACIÓN PROFESIONAL · MARKETING DIGITAL · UNIDAD 5

Seguridad y continuidad

Lunes 17 de mayo de 2027. Unai ha instalado un antivirus: «Ya estamos protegidos». El martes llega un correo que imita a la pasarela de pago y el antivirus no avisa; el miércoles, en un simulacro, se da por perdido el catálogo de kits. ¿En cuánto tiempo se recupera y con qué datos?

PARA EMPEZAR

En esta unidad aprenderás a…

- Distinguir programas maliciosos, fraudes, suplantaciones, errores humanos y fallos técnicos, y reconocer sus señales sin abrir nada peligroso.
- Asignar permisos con mínimo privilegio y separación de funciones, y comprobarlos con un usuario de prueba.
- Relacionar cada barrera de seguridad con la amenaza que reduce y con lo que no cubre.
- Diseñar un plan de copias con versiones y demostrar que una copia se puede restaurar y abrir.
- Responder a un incidente con detección, contención, verificación por un canal independiente y registro.
- Calcular los datos en riesgo y el tiempo ideal de una restauración con sus unidades.

SITUACIÓN DE PARTIDA

«Ya estamos protegidos: si entra algo raro, lo para»

Lunes 17 de mayo de 2027. Unai ha instalado un programa de protección en el portátil de la trastienda y en la tableta del mostrador de **La Despensa de Nora** (caso ficticio). Nora no lo discute, pero llama a Idaira, la técnica de sistemas que les da soporte: quiere un simulacro para el miércoles. «Si mañana perdemos el catálogo de kits, ¿en cuánto tiempo lo tenemos otra vez y con qué datos?»

El **martes 18 a las 9:40** llega un correo que parece de la pasarela de pago: «Su cuenta de abono será suspendida hoy. Confirme sus datos bancarios en el enlace». El antivirus no avisa de nada. El **miércoles 19 a las 15:00**, en el simulacro, Idaira da por perdido el catálogo interno de kits; la última copia es de las **23:00 del martes**.

❓ ¿Qué debe decidir o comprobar Nora en esta situación?

❓ ¿Qué sabemos del correo del martes y qué estamos suponiendo?

❓ ¿Qué prueba permitiría saber si la copia del martes sirve de verdad?

❓ ¿Quién debería poder cambiar la cuenta donde la tienda cobra sus ventas?

MAPA DE LA UNIDAD

Lo que vamos a ver

5.1 Amenazas y señales

5.2 Control de acceso

5.3 Actualización y barreras

5.4 Copias y restauración

5.5 Respuesta y documentación

La copia está hecha. ¿La has recuperado?



La copia está hecha.

¿La has podido recuperar?





Vamos a comprobarlo ahora. En otra carpeta, sin pisar el original.

CLAVE

Una copia que nunca se ha restaurado es una esperanza, no una garantía. Se comprueba restaurándola en una carpeta de pruebas, abriéndola y registrando el resultado.

Cinco familias de amenazas

Una **amenaza** es cualquier cosa que puede dañar la confidencialidad, la integridad o la disponibilidad de la información. Cada familia se combate de forma distinta.

FAMILIA	QUÉ ES	EJEMPLO EN LA DESPENSA
Programa malicioso	Virus, programa espía (*spyware*), troyano o de secuestro	Un «albarán» comprimido que instala un programa espía
Fraude	Engaño para obtener dinero o datos	Factura de un proveedor que no existe
Suplantación	Alguien se hace pasar por otro de confianza	Correo que imita a la pasarela de pago
Error humano	Equivocación de una persona, sin mala intención	Guardar encima del catálogo una versión antigua
Fallo técnico	Avería o caída de un equipo o servicio	El disco de red no arranca un lunes

CLAVE

Confidencialidad: que solo la vea quien debe. **Integridad**: que no se altere sin control. **Disponibilidad**: que esté cuando hace falta.

5.1 · DOCUMENTO 1

El correo del martes, con las seis señales

Martes 18/05/2027, 9:40 (ficticio). Se analiza **sin pulsar el enlace**, sin descargar nada y sin responder.

SEÑAL	QUÉ SE MIRA	EN EL CORREO DEL MARTES
Remitente	La dirección completa y su dominio, no el nombre visible	`pasarela-verificacion.example`; la real escribe desde `pasarela.example`
Responder a	Si las respuestas van a otra dirección	`soporte.cobros@correo-rapido.example`
Urgencia	«Hoy mismo», «será suspendida»	«URGENTE: confirme hoy sus datos bancarios…»
Enlace	La dirección real, con el puntero encima	Muestra `panel.pasarela.example`; lleva a `pasarela-verificacion.example/acceso`
Petición	Contraseñas o datos bancarios desde un enlace	Cambiar la cuenta de abono
Procedimiento	Lo que dice el contrato	Cambios solo en el panel y con aprobación de Nora

Adjuntos: ninguno. Es una **suplantación con fin de fraude**: el antivirus no tiene nada que analizar. Engañar a una persona en vez de a una máquina es **ingeniería social**; por correo, su forma más común es el **phishing**.

CLAVE

Analizar sin abrir: dirección completa, «Responder a» y destino real del enlace; se guarda el mensaje como prueba y se avisa a quien corresponda.

🙋 PREGUNTA PARA LA CLASE

El correo del martes no lleva adjuntos y el antivirus no avisa de nada. ¿Qué es?

A Un correo seguro: el antivirus lo habría parado

B Una suplantación con fin de fraude (ingeniería social)

C Un fallo técnico de la pasarela

✔ Remitente de otro dominio, «Responder a» de un tercero, urgencia, enlace que no coincide, petición de datos bancarios y fuera del procedimiento. No hay programa que analizar: lo frenan el procedimiento y la verificación por un canal independiente (autoevaluación 1).

Quién entra, qué ve y qué puede cambiar



Identificación

Decir quién eres: el usuario `unai`.



Autenticación

Demostrarlo: contraseña, código en el móvil. Con **doble factor**, algo que sabes y algo que tienes: una contraseña robada no basta.



Autorización

Lo que el sistema te deja hacer dentro: leer, editar, aprobar. Una contraseña fuerte no arregla una autorización mal hecha.



Mínimo privilegio y separación de funciones

Cada persona, solo los permisos que necesita para su tarea; una operación delicada, entre dos: **quien propone no aprueba**.

CLAVE

Cambiar la cuenta de abono lo **propone Unai** (sin poder aplicarlo) y lo **aprueba Nora**, que firma el contrato con la pasarela: un solo engaño no basta para desviar los cobros.

5.2 · DOCUMENTO 2

La matriz de accesos de La Despensa

L = leer, E = editar, A = aprobar, P = proponer un cambio sin aplicarlo, — = sin acceso (ficticia).

PERSONA	CATÁLOGO	PEDIDOS Y FACTURAS	CLIENTES	PASARELA
Nora	L, E, A	L, E, A	L, E	L, A
Unai	L, E	L (pedidos)	L (lista)	L (pedidos), P
Itxaso	L, E	L, E (pedidos)	L (entrega)	—
Adrián	L	—	—	—
Idaira	L, E (soporte)	— (solo con aviso)	—	—

Permisos efectivos: lo que el sistema deja hacer de verdad. Con el usuario de prueba `prueba.catalogo`, en ensayo: una acción permitida (editar una ficha de kit) y una denegada (abrir facturas); se anota con fecha y hora y, al acabar, se desactiva.

CLAVE

Cuentas personales: con una cuenta compartida («tienda») el registro no dice quién hizo cada cambio. Las bajas, el mismo día; las contraseñas, en un gestor de contraseñas.

Cada barrera tapa un hueco: ninguna los tapa todos

BARRERA	QUÉ REDUCE	QUÉ NO CUBRE
Actualizaciones	Ataques a fallos ya conocidos	Engaños a personas
Antivirus	Virus y programas espía	Correos sin adjunto, errores, averías
Cortafuegos	Conexiones no autorizadas entre redes	Lo que entra por un enlace pulsado
Filtro y autenticación del correo	Remitentes falsificados	Un dominio parecido del atacante
Doble factor	Entrar con una contraseña robada	Lo que haga un usuario legítimo
Copias con versiones	Pérdida de datos	Que los datos se vean

El cortafuegos del router separa la red del personal, la de invitados y la del datáfono. Actualizar: pronto, primero en ensayo y con copia previa; lo que ya no recibe actualizaciones se sustituye.

CLAVE

Defensa en capas: si una barrera falla, la siguiente frena el daño.

5.3 · TABLA 1

El registro de riesgos: probabilidad × impacto

P e I, de 1 a 3. Riesgo de 6 a 9, **alto**; de 3 a 4, **medio**; de 1 a 2, **bajo** (ficticio; mayo de 2027).

AMENAZA	P	I	RIESGO (P × I)
Correo que suplanta a la pasarela	3	3	9 · alto
Cuenta compartida del panel de la tienda	3	2	6 · alto
Catálogo interno sobrescrito por error	2	2	4 · medio
Actividad 9: acceso indebido al panel, con cuentas personales y doble factor	1	2	**2 · bajo**

En la actividad 9 baja la probabilidad, no el impacto: si alguien llegara a entrar, el daño posible sería el mismo.

CLAVE

Los riesgos altos no los frena el antivirus. Lo que queda tras las barreras es el **riesgo residual**: nunca es cero.

Qué es una copia útil



Útil si…

Está **completa**, es **reciente**, tiene **versiones** (por si el daño se copió) y está en una **ubicación controlada**.



Tipos

Completa: todo. **Incremental**: lo cambiado desde la última copia de cualquier tipo. **Diferencial**: lo cambiado desde la última completa.



Regla 3-2-1

Buena práctica, no obligación legal: **tres** copias (original, diaria, semanal) en **dos** soportes y **una** fuera de la empresa.



RPO y RTO

Pérdida máxima tolerable (RPO): cuánto trabajo, en tiempo, se acepta perder. **Tiempo de recuperación** (RTO): cuánto puede estar parado el servicio.

CLAVE

Supuesto de la actividad 12 (el plan real hace copias completas): completa el domingo y restauración el jueves; con incrementales, la completa y las de lunes, martes y miércoles; con diferencial, la completa y la del miércoles (actividad 12).

5.4 · DOCUMENTO 3

El plan de copias de La Despensa

Versión 1.2, mayo de 2027 (ficticio).

QUÉ	DÓNDE	CUÁNDO	VERSIONES
Original de trabajo	Nube con versiones (servicio genérico)	Al guardar	Historial del servicio
Copia diaria completa	Disco de red de la trastienda	Cada día a las 23:00	7 diarias
Copia semanal cifrada	Nube de copias, fuera de la tienda	Domingo a las 23:30	4 semanales
Prueba de restauración	Carpeta de pruebas	Una vez al mes	Registro en el dossier

7 + 4 = **11 versiones**. Las cuatro semanales de la carpeta compartida (12 GB) ocupan 4 × 12 = **48 GB** en la nube.

CLAVE

La copia del disco de red, «que está aquí al lado», no basta sola: las tres copias son el original, la diaria y la semanal, y la semanal cifrada está **fuera de la tienda**, como pide la regla 3-2-1.

Los datos en riesgo del simulacro

Datos en riesgo = incidente − última copia

Del martes 18/05 a medianoche	23:00 → 24:00	**1 h**
Del miércoles 19/05	0:00 → 15:00	**15 h**
Total sin cubrir por la copia diaria	1 + 15	**16 h**
Con otra copia diaria a las 14:00	14:00 → 15:00	**1 h**

El historial de versiones de la nube puede ayudar a rehacer los cambios, pero solo si se comprueba que esas versiones existen y están completas. Nora pide, de momento, anotar los cambios de precios para poder rehacerlos.

CLAVE

No son 8 h: de las 23:00 a las 15:00 del día siguiente hay **16 h** (autoevaluación 6).

5.4 · EJEMPLO

El tiempo ideal de una restauración

Tamaño en bits ÷ velocidad en bits por segundo (1 byte = 8 bits; 1 GB = 1.000 MB), sin pausas ni otros usos de la línea.

QUÉ SE RESTAURA Y POR DÓNDE	CÁLCULO	TIEMPO IDEAL
Catálogo, 38 MB, fibra de 100 Mbps	38 × 8 ÷ 100	3,04 s
Catálogo, 38 MB, respaldo de 30 Mbps	38 × 8 ÷ 30	10,13 s
Carpeta, 12 GB, fibra de 100 Mbps	12.000 × 8 ÷ 100	960 s = 16 min
Carpeta, 12 GB, respaldo de 30 Mbps	12.000 × 8 ÷ 30	53,33 min
Actividad 11: carpeta de 12,6 GB (+5 %), fibra	12.600 × 8 ÷ 100	1.008 s = 16,80 min

La fibra supone bajar de la nube; desde el disco de red el tiempo es otro: se mide.

CLAVE

El tiempo ideal no es una promesa: el real se mide en la prueba. En el simulacro, 7 min (buscar la versión, restaurar y abrir).

Cómo se demuestra que una copia sirve

Registro 1 · Prueba del 19/05/2027: diaria del 18/05, 23:00, en la carpeta de pruebas del disco de red.

1. **Elegir copia**
   Fecha y versión.
2. **Restaurar aparte**
   En una carpeta de pruebas, nunca encima del original.
3. **Abrir y comprobar**
   46 fichas, precios y alérgenos del martes.
4. **Integridad y permisos**
   La huella igual a la del día 18 (el tamaño no basta); solo la abre el equipo.
5. **Medir y registrar**
   7 min · Idaira y Unai · correcta · próxima prueba el 16/06/2027.

CLAVE

La norma dice: RGPD, art. 32.1: las medidas incluyen «la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico» y «un proceso de verificación, evaluación y valoración regulares».

Las seis fases de la respuesta

Proporcional: no se apaga la tienda por un correo sospechoso, pero no se ignora.



Detectar

Ver la señal y avisar enseguida a quien corresponde.



Contener

No pulsar ni responder, bloquear, cambiar la contraseña, aislar.



Verificar

Por un canal independiente: el teléfono del contrato.



Recuperar

Desde una copia comprobada, si hay daño.



Registrar

Qué pasó, qué se hizo y quién; guardar pruebas.



Aprender

Qué barrera faltó y qué cambia.

CLAVE

Nunca se verifica con el teléfono o el enlace del correo: lo que trae el mensaje lo controla quien lo envió.

5.5 · DOCUMENTO 4

El registro INC-2027/014

CAMPO	CONTENIDO
Detección	18/05/2027, 9:40 · Unai · correo que pide confirmar la cuenta de abono
Tipo	Suplantación de la pasarela con fin de fraude; sin adjunto
Contención	Enlace sin pulsar; remitente bloqueado; aviso al equipo a las 9:55
Verificación	10:05 · Nora llama al teléfono del contrato: la pasarela no lo envió
Pruebas y datos	Correo con cabeceras guardado; ningún dato personal afectado
Mejora y cierre	Doble factor en el panel · Nora · cerrado a las 12:00

Un intento de phishing sin consecuencias no tiene nada que restaurar. El correo no se borra: se guarda con sus cabeceras como prueba.

CLAVE

Para saber más: el INCIBE atiende el **017**, su línea de ayuda en ciberseguridad, y publica guías para empresas.

Violación de la seguridad de los datos personales



Ante datos de personas perdidos, alterados o vistos sin autorización, notificar a la autoridad de control «sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella», salvo que sea improbable el riesgo para las personas. Art. 33.5: documentar «cualquier violación de la seguridad de los datos personales».

Reglamento (UE) 2016/679 (RGPD), de 27 de abril de 2016, art. 33.1 y 33.5 · Consulta la versión vigente

SUJETO OBLIGADO

La empresa que trata los datos (en La Despensa, la lista de clientes y los contactos de las oficinas): documenta siempre la violación, aunque parezca leve, y valora el riesgo para las personas afectadas.

NO OBLIGA A…

…a notificar un incidente sin datos personales: INC-2027/014 se documenta, pero nadie escribió ni vio datos personales (actividad 15).

CLAVE

Cambiaría si se hubiera accedido al panel con datos de clientes o a la lista de correo: entonces se valora el riesgo y se notifica en 72 h salvo que sea improbable.

CASO RESUELTO · PASO A PASO

El correo de la cuenta de abono y la copia del catálogo



Idaira, Nora y Unai

Martes 18 y miércoles 19 de mayo de 2027: el correo de las 9:40 y el simulacro de las 15:00 con el catálogo de kits (38 MB). Caso ficticio.

1. **La decisión y los datos.** ¿Se cambia la cuenta de abono? ¿Recupera el catálogo la copia del martes? Documento 1, contrato con la pasarela (cambios solo en el panel, con aprobación de la gerencia) y copia de las 23:00 del 18/05.

2. **El correo.** Dominio distinto, «Responder a» de un tercero, enlace a otro dominio, fuera del procedimiento. Nora llama al teléfono del contrato a las 10:05: la pasarela no lo envió. Se bloquea el remitente, se guarda el correo y se abre INC-2027/014.

3. **La restauración.** De las 23:00 a las 15:00: 1 + 15 = 16 h en riesgo. Ideal de referencia (nube a 100 Mbps; del disco de red se mide): 38 × 8 = 304 Mb; 304 ÷ 100 = 3,04 s. Idaira restaura en la carpeta de pruebas; Unai abre, comprueba fichas y precios y compara la huella. Los cambios del miércoles se rehacen (el historial de la nube puede ayudar).

4. **Qué se concluye y qué no.** El correo era una suplantación: lo demuestra la llamada, no el antivirus. La restauración demuestra que esa copia se abre y está completa; no que lo estén las demás ni que el tiempo real sea de 3 segundos.

✔ **Enlace sin usar y registro INC-2027/014 con pruebas; catálogo recuperado de la copia de las 23:00 en una carpeta de pruebas (16 h en riesgo). Se activa el doble factor en el panel y la prueba se repetirá cada mes.**

🙋 PREGUNTA PARA LA CLASE

Ojo profesional. El informe semanal de Unai dice: «La copia diaria de las 23:00 se hace bien: marca en verde. No ha hecho falta restaurarla nunca». ¿Qué falla?

A Nada: si marca en verde, la copia sirve

B Una copia no está comprobada hasta restaurarla aparte, abrirla y registrarla; y el 19/05 ya se restauró

C Que debería hacerse a las 14:00

✔ El verde dice que se copió lo configurado, no todo lo que hace falta (Lectura: la tienda volvió sin fotos). Los otros errores del informe: cambiar la cuenta desde el enlace, el catálogo con acceso a cobros, la cuenta compartida y las «8 h» que son 16 h.

D05 · Prueba de recuperación

Para tu dossier de comprobaciones (servicio de kits de La Despensa u otra empresa aprobada):

1. **Accesos**
   Matriz de accesos con un permiso denegado comprobado con usuario de prueba.
2. **Barreras**
   Lista de barreras activadas, con fecha.
3. **Copia**
   Copia restaurada en carpeta de pruebas y abierta, con el tiempo medido.
4. **Incidente**
   Registro INC simulado con sus seis fases.

CLAVE

Ninguna contraseña visible; la restauración no pisa el original; cada prueba con fecha y responsable. Lo que no hayas demostrado, anótalo como **«sin demostrar»**.

APRENDE CON LA IA

La respuesta que recibió Unai

Unai preguntó a un asistente de IA cómo saber si las copias de La Despensa sirven. Pulsa cada tarjeta.

«Tener una copia demuestra que podrás restaurarla»

BULO

Solo lo demuestra haberla restaurado en otra carpeta, abierto y comprobado (contenido, integridad, versión y permisos).

«Si el programa marca la tarea en verde, los archivos están a salvo»

BULO

El verde quería decir que se copió lo configurado: la tienda de ensayo volvió sin fotos.

«Abrir la copia solo añade riesgo de estropearla»

BULO

Se restaura en una carpeta de pruebas, sin pisar el original: abrirla allí no estropea nada.

«Con copia y antivirus, la continuidad está garantizada»

BULO

Nada la garantiza: queda un riesgo residual y lo no probado se escribe «sin demostrar».

REPASO

Ideas clave

- Cinco familias de amenazas: programa malicioso, fraude, suplantación, error humano y fallo técnico; cada una se combate distinto.
- El correo del martes es ingeniería social sin adjunto: el antivirus no tiene nada que analizar.
- Los permisos efectivos se comprueban con un usuario de prueba: una acción permitida y una denegada.
- Copia útil: completa, reciente, con versiones y en ubicación controlada; regla 3-2-1.
- Respuesta: detectar, contener, verificar por canal independiente, recuperar, registrar y aprender; con datos personales, RGPD art. 33.
- Un mensaje sospechoso se analiza sin abrir: remitente, «Responder a», urgencia, enlace real, petición y procedimiento.
- Identificación, autenticación y autorización son pasos distintos; mínimo privilegio y quien propone no aprueba.
- Cada barrera reduce una amenaza y deja huecos: defensa en capas y riesgo residual, nunca cero (riesgo = P × I).
- Datos en riesgo: de las 23:00 a las 15:00, 16 h. Tiempo ideal de referencia (nube): 38 × 8 ÷ 100 = 3,04 s; el real se mide (7 min).



¡Ahora te toca a ti!

Repasa, practica y comprueba lo que has aprendido.

📝 **Resumen**

✅ **Test**

👆 **Interactivos**

Libro, presentaciones, resúmenes y tests gratis en **josesande.com**