6 semanas | Hasta 15 participantes | Claude Code o Codex | Capacitación de seguridad informática

Seguridad informática para pymes, con agentes de guardia

Ordená la seguridad de tu pyme sin área de sistemas. Agentes de guardia revisan cada semana una lista de chequeo y una persona aprueba.

PARA QUIÉN

Dueños, gerencia, administración y finanzas de pymes sin área de sistemas, y la persona que hoy "se encarga de la computación".

CÓMO TRABAJAN LOS AGENTES DE IA

Los agentes de guardia (Claude o Codex, a elección de la organización) revisan cada semana una lista de chequeo y reportan a una persona. Esa persona aprueba cualquier cambio. Los agentes solo leen y avisan; no modifican nada por su cuenta.

Soporte incluido: Todas las capacitaciones incluyen 3 meses de soporte, ayuda y acompañamiento ante dudas, desde la última clase.

Lo que te llevas

- Inventario de activos y accesos de tu organización.
- Protocolo de incidente de una página y guía de estafas con IA para tu equipo.
- Clasificación de activos por criticidad y plan de copias 3-2-1 con restauración probada.
- Claves, doble factor y copias de seguridad probadas con una restauración real.
- Agentes de guardia funcionando, con su lista de chequeo semanal y la rutina trimestral.
- Tablero de indicadores para la dirección y presupuesto de seguridad ordenado por riesgo.

Dicta Julián Bagilet

Más de 19 años en tecnología. Estudio de software en Villa General Belgrano, Córdoba.

Temario

1

SEMANA 1 SEGURIDAD

Inventario de activos y accesos

Qué equipos, cuentas y servicios tenés, quién accede a cada uno y a quién se le quitó el acceso al irse.

QUÉ VEMOS

- Cómo listar equipos, cuentas de correo, bancos, sistemas y servicios en la nube sin que se escape nada.
- Quién tiene acceso a qué: la cuenta que comparten tres personas y el usuario de alguien que ya se fue.
- Cómo quitar accesos cuando alguien deja la organización: una lista corta de salida que se usa siempre.
- Qué cuenta haría más daño si se pierde: el correo del dueño, el banco o el sistema de facturación.
- Cómo clasificar los activos por criticidad: cuánto tiempo puede estar caído cada sistema y cuánto dato se puede perder sin que el negocio se detenga.

Al terminar la semana: Tu equipo termina con el inventario de activos y accesos, y con la lista de accesos viejos para dar de baja.

2

SEMANA 2 SEGURIDAD

Claves y doble factor

Gestor de claves, doble factor en las cuentas críticas y cuentas compartidas bajo control. Se aplica en tu organización, con tu equipo.

QUÉ VEMOS

- Qué es un gestor de claves y por qué es mejor que la libreta, el Excel o el papelito pegado al monitor.
- Doble factor explicado simple: además de la clave, una confirmación en el celular. Qué cuentas lo necesitan primero.
- Cuentas compartidas: cómo pasar de una clave que sabe todo el mundo a accesos propios o a un uso controlado.
- Cómo se aplica con tu equipo en la sala, cuenta por cuenta, empezando por el correo y el banco.
- Cuentas de administración separadas de las de uso diario, y por qué el dueño no debería leer el correo con la cuenta que puede cambiarlo todo.
- Una bóveda de claves compartida con permisos por persona, en lugar de la planilla o el grupo de WhatsApp.

Al terminar la semana: Tu equipo termina con el gestor de claves en uso y el doble factor activado en las cuentas más críticas.

Temario (continuación)

3

SEMANA 3 · SEGURIDAD

Copias que se restauran

Qué se copia, dónde y cada cuánto. Se hace una restauración de prueba. Se ordenan las actualizaciones de equipos y programas.

QUÉ VEMOS

- Qué copiar: planillas, facturación, fotos y documentos. Los programas se pueden reinstalar y no son la prioridad.
- Por qué conviene tener más de una copia en lugares distintos, una de ellas fuera de la oficina y sin conexión permanente.
- Una restauración de prueba real: recuperar un archivo borrado y ver cuánto tarda, porque una copia sin probar no es una copia.
- Actualizaciones: quién las aprueba, cada cuánto y qué hacer con el equipo viejo que ya no las recibe.
- La regla 3-2-1: tres copias, en dos tipos de soporte, una fuera de la oficina y una que no se pueda modificar. Qué significa en tu caso.
- Por qué el ransomware también cifra la copia conectada, y qué copia aislada te permite volver.

Al terminar la semana: Terminan con un plan de copias escrito, una restauración de prueba hecha y un calendario de actualizaciones.

4

SEMANA 4 · SEGURIDAD

Correo, phishing y estafas con IA

Cómo reconocer phishing, voz clonada, deepfake y fraude del CEO. Verificación por un segundo canal y palabra clave.

QUÉ VEMOS

- Cómo reconocer un mail falso hoy: sin faltas de ortografía, con el logo correcto y un pedido que parece razonable.
- Estafas con voz clonada, videos falsos y fraude del CEO: cómo suenan y qué pregunta rompe el engaño.
- La regla de oro: ante un pedido de dinero o de datos, se verifica por otro canal ya conocido, nunca respondiendo al mismo mensaje.
- La palabra clave interna y qué hacer si alguien ya hizo clic o pagó. La demostración usa la voz del instructor, con su consentimiento.
- El correo de la organización: SPF, DKIM y DMARC explicados sin jerga, reglas de reenvío ocultas y avisos de inicio de sesión inusual.
- Cómo capacitar al personal en 20 minutos por trimestre: ejemplos reales de pedidos urgentes y qué hacer ante la duda.

Al terminar la semana: Tu equipo termina con una guía de estafas con IA de una página y la palabra clave interna acordada.

Temario (continuación)

5

SEMANA 5 SEGURIDAD

Protocolo de incidente y agentes de guardia

Redactamos el protocolo de una página y configuramos los agentes de guardia con su lista de chequeo semanal y una persona que aprueba.

QUÉ VEMOS

- Cómo se escribe el protocolo de incidente de una página: qué apagar, a quién llamar y quién decide.
- Qué es un agente de guardia: un asistente que cada semana repasa una lista y te cuenta qué encontró.
- Qué revisa la lista semanal: cuentas sin doble factor, copias que no corrieron, equipos sin actualizar y accesos de personas que se fueron.
- Por qué solo lee y avisa: los cambios los aprueba una persona y cada revisión queda registrada.
- Cómo hacer que el agente de guardia corra solo, programado, sin que nadie se lo pida. Y qué pasa si una semana no corre: tiene que avisar que no corrió.
- El laberinto de señuelos: tablas, funciones y claves trampa con datos inventados que ningún usuario real necesita. Si alguien las toca queda registrado con la hora del servidor y llega un aviso. Detectan y dejan evidencia, no contraatacan. Se enseña con ejemplos genéricos de tu propio sistema.
- Dispositivos y terceros: cifrado de disco, bloqueo remoto de un notebook perdido, y qué acceso tienen tu contador, tu proveedor de sistemas y tu proveedor de internet y cómo se revisa.

Al terminar la semana: Tu equipo termina con el protocolo escrito y los agentes de guardia configurados, con la persona que aprueba ya definida.

6

SEMANA 6

Primer reporte y rutina trimestral

Revisamos el primer reporte de los agentes, ajustamos y cerramos con la rutina trimestral para sostenerlo sin nosotros.

QUÉ VEMOS

- Cómo leer el primer reporte: qué es urgente, qué puede esperar y qué fue un falso aviso.
- Cómo ajustar la lista de chequeo para que avise lo que importa sin llenar la bandeja de ruido.
- La rutina trimestral: qué se revisa cada tres meses, quién lo hace y cómo se deja constancia.
- Cómo seguir sin el estudio: qué hacer si cambia la persona responsable o se suma una herramienta nueva.
- Los indicadores para la dirección: porcentaje de cuentas con doble factor, copias restauradas con éxito, accesos dados de baja y tiempo de cierre de cada hallazgo.
- Qué conviene primero con poco presupuesto: ordenar las medidas por riesgo evitado y por esfuerzo, y qué esperar al año siguiente.

Al terminar la semana: Terminan con el primer reporte revisado, la lista de chequeo ajustada y la rutina trimestral con responsables.

Seguridad y alcance

Seguridad incluida en este programa

- Agentes de guardia con permisos de solo lectura: revisan y avisan, no cambian nada.
- Claves y datos sensibles fuera de lo que ve el agente.
- Agentes de guardia programados que corren solos y avisan si una semana no corrieron; señuelos que dejan evidencia.
- Copias con una versión aislada que el ransomware no alcanza, y bóveda de claves con permisos por persona.
- Una persona aprueba cada cambio que proponga un agente.
- Registro de cada revisión semanal, guardado y revisable.
- Doble factor y palabra clave interna ante pedidos urgentes de dinero.

Qué no se enseña ni se hace

- No incluye pruebas de intrusión de red, certificaciones ni asesoramiento legal.
- No se clonan voces de personas reales: la demostración usa la voz del instructor, con su consentimiento.
- No se envía phishing a tus empleados sin autorización escrita y aviso previo a la dirección.

Requisitos

Una persona responsable que apruebe los cambios y un plan pago de Claude o de Codex a cargo de la organización. No hace falta saber de sistemas.

Inversión y formas de pago

Programa completo

$ 8.500.000

Precio del programa completo, en pesos argentinos, hasta 15 participantes. Anticipo del 50% al confirmar, saldo al finalizar. No incluye el plan pago de Claude o Codex.

Valores en pesos argentinos.

mercado pago

PAGO **Transferencia o Mercado Pago**
Anticipo del 50% al confirmar y saldo al finalizar. Se acuerda por escrito.

FACTURA Se emite factura por cada pago. El tratamiento de IVA se informa en la propuesta.

Cómo inscribirte

1. **Escribinos**
Contanos qué querés lograr por WhatsApp.

2. **Confirmamos cupo y fecha**
Te avisamos apenas hay fecha y lugar en la cohorte.

3. **Reservá tu lugar**
Elegís cuotas o transferencia y recibís la confirmación por escrito.

WhatsApp +54 9 3546 54-6063

julianbagilet.com/capacitaciones/ · Instagram @mangopips_ok · Villa General Belgrano, Córdoba

Condiciones

Valores vigentes hasta el 31 de enero de 2027. Certificado de aprobación del estudio de Julián Bagilet, sin validez oficial. Derecho de arrepentimiento de 10 días corridos en compras a distancia por personas (Ley 24.240, art. 34). Si una cohorte no llega al mínimo de inscriptos, se reprograma o se devuelve el 100% de lo abonado. Los casos de las clases se explican como patrones, sin nombres ni datos de clientes.