HumanOS

ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

HUMANOS MANAGER GUIDE

CÓMO CONVERTIR EL RIESGO HUMANO EN UNA CAPACIDAD DE SEGURIDAD

5 RIESGOS
Qué revisar.

5 HÁBITOS
Qué instalar.

5 MÉTRICAS
Qué medir.

30 DÍAS
Cómo empezar.

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

EL NUEVO ENFOQUE
DE CAPACITAR USUARIOS
A GESTIONAR RIESGO HUMANO

La concientización no debería terminar en:
CAPACITACIÓN - EXAMEN - CERTIFICADO - LISTO
Las amenazas cambian. El phishing cambia. La ingeniería social cambia.
La IA cambia. Los canales cambian.

LA PREGUNTA DEL MANAGER

NO	***SI***
¿Cuántos empleados capacité?	¿Qué tan preparada está mi organización para reconocer, resistir, reportar y responder cuando una amenaza llega a una persona?

TU EQUIPO TAMBIÉN ES PARTE DE TU SUPERFICIE DE ATAQUE.

Tu organización puede contar con firewall, EDR/XDR, SIEM, MFA, SOC, backups y controles de acceso. Pero existe otra superficie que evoluciona todos los días:

LAS PERSONAS



PERSONAS
Reconocen y reportan.



PROCESOS
Contienen y validan.



TECNOLOGÍA
Detecta y responde.

siscotec
30 AÑOS
Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

LOS 5 RIESGOS QUE DEBERÍA REVISAR UN MANAGER

No necesitas revisar todo al mismo tiempo. Empieza por estas cinco áreas.



01 IDENTIDAD COMPROMETIDA

El atacante puede intentar entrar como un usuario legítimo.

REVISA: MFA en cuentas críticas · cuentas privilegiadas · accesos excesivos · usuarios inactivos · cuentas compartidas · revisiones periódicas · métodos resistentes al phishing cuando sean viables.

PREGUNTA: ¿Podemos saber rápidamente si una identidad legítima está siendo utilizada de manera anómala?



INGENIERÍA SOCIAL 02

CONFIANZA - AUTORIDAD - URGENCIA - ACCIÓN

REVISA: Phishing · Smishing · Vishing · Suplantación ejecutiva · MFA fatigue · Deepfakes · Solicitudes financieras fuera de procedimiento.

PREGUNTA CLAVE: ¿Nuestro equipo sabe cuándo una solicitud aparentemente legítima requiere verificación adicional?



03 ERRORES SIN CAPACIDAD DE RECUPERACIÓN

El riesgo humano no termina en la nómina

REVISA: quién tiene acceso · nivel de acceso · duración · autenticación · revocación · salida del tercero.

PREGUNTA: ¿Tenemos el mismo nivel de control sobre las identidades externas que sobre las internas?



04 PROCESOS QUE DEPENDEN DE LA CONFIANZA

"Me lo pidió el gerente." · "El proveedor llamó." · "Ya lo autorizó alguien."

REVISA: transferencias · cambios de cuentas bancarias · pagos · accesos privilegiados · creación de usuarios · recuperación de cuentas · cambios de proveedores · información confidencial.

PREGUNTA: ¿Qué procesos críticos pueden ejecutarse únicamente porque alguien parece confiable?



05 · TERCEROS Y ECOSISTEMA

El riesgo humano no termina en la nómina.

REVISA: quién tiene acceso · nivel de acceso · duración · autenticación · revocación · salida del tercero.

PREGUNTA: : ¿Tenemos el mismo nivel de control sobre las identidades externas que sobre las internas?

siscotec

30 AÑOS
Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

LOS 5 HÁBITOS QUE DEBERÍA INSTALAR EL MANAGER

No necesitas revisar todo al mismo tiempo. Empieza por estas cinco áreas.

01

No actuar automáticamente frente a:
Urgencia · autoridad · presión · solicitudes inesperadas.
REGLA: SI TE PRESIONA PARA ACTUAR, TE DA UNA RAZÓN PARA VERIFICAR.



PAUSAR

02

no es desconfiar.
Debe formar parte del proceso.
Especialmente cuando existe:
DINERO + IDENTIDAD + ACCESO + INFORMACIÓN SENSIBLE



VERIFICAR

03

Debe ser: FÁCIL · RÁPIDO · SIN MIEDO
"Gracias por reportarlo. ¿Qué ocurrió?"



REPORTAR

04

no significa solamente instalar software. También significa actualizar:
CONOCIMIENTO + PROTOCOLOS + CONTROLES + COMPORTAMIENTOS



ACTUALIZAR

05

Cada intento o incidente debería generar un aprendizaje:
¿Qué ocurrió? ¿Por qué funcionó? ¿Qué control falló? ¿Qué comportamiento debemos reforzar? ¿Qué podemos cambiar?



APRENDER

siscotec 30 AÑOS Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

NO MIDAS CAPACITACIÓN. *MIDE PREPARACIÓN*

Completar una capacitación demuestra participación. No necesariamente demuestra preparación. Por eso, un manager debería observar al menos cinco indicadores.



01 · REPORT RATE

¿Cuántas personas reportan amenazas sospechosas?
No medir solamente quién hizo clic.
Medir también: ¿Quién detectó y reportó?

02 · TIME TO REPORT

¿Cuánto tiempo pasa desde la detección hasta el reporte?
Menor tiempo de reporte = mayor oportunidad de respuesta.

03 · PHISHING RESILIENCE

No mirar únicamente el porcentaje de clics. Considerar:
Interacción + reporte + dificultad del escenario + reincidencia + evolución.

04 MFA ANOMALIES

Solicitudes MFA no iniciadas. -Intentos repetidos. - Bloqueos. - Autenticaciones anómalas.
PREGUNTA CLAVE: ¿Estamos detectando señales tempranas de compromiso de identidad?

05 · HUMAN RISK TREND

La pregunta estratégica no es: "¿Estamos seguros?" Es: ¿ESTÁ DISMINUYENDO NUESTRO RIESGO HUMANO?

Comparar periódicamente: Phishing · Identidad · Reportes · Errores · Tiempo de respuesta · Reincidencia

siscotec
30 AÑOS
Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

HUMANOS DASHBOARD

DEJA DE MEDIR ACTIVIDAD. EMPIEZA A MEDIR EVOLUCIÓN.

Indicador	Actual	Objetivo	Tendencia
Report Rate	XX%	Definido internamente	↑ ↓
Time to Report	XX min	Definido internamente	↑ ↓
Phishing Resilience	XX%	Definido internamente	↑ ↓
MFA Anomalies	XX	Definido internamente	↑ ↓
Human Risk Trend	XX	↓	↑ ↓

IMPORTANTE

No existen objetivos universales. Cada organización debe definir sus referencias según: Tamaño · exposición · criticidad · madurez · industria.

NO ENTRENES A TODOS DE LA MISMA MANERA

EL RIESGO NO ES IGUAL PARA TODOS

Una estrategia madura adapta el entrenamiento al rol y a la exposición.

ROL	PRIORIDADES
Usuario general	Phishing · MFA · credenciales · reporte
Finanzas	BEC · transferencias · cambios de cuenta · suplantación
TI	Privilegios · credenciales · accesos · endpoints
Dirección	Deepfakes · suplantación ejecutiva · fraude · información sensible
Administradores	Privilegios elevados · identidad · MFA resistente al phishing · respuesta

PREGUNTA PARA EL MANAGER

¿Estamos capacitando a las personas según su riesgo o estamos entregando el mismo contenido a todos?

siscotec 30 AÑOS Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

DE CAPACITACIÓN A CULTURA

LA CULTURA NO SE DECLARA. SE CONSTRUYE.



CAPACITAR
"Les enseñamos qué reconocer."

PRACTICAR
"Simulamos situaciones reales."

MEDIR
"Observamos comportamiento."

CORREGIR
"Adaptamos capacitación y controles."

INTEGRAR
"Lo incorporamos a procesos y operaciones."

CULTURA
La seguridad forma parte de la manera habitual de trabajar.

HUMANOS SECURITY LOOP

UN CICLO CONTINUO DE ACTUALIZACIÓN

HumanOS propone convertir el riesgo humano en un ciclo permanente:



siscotec
30 AÑOS
Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

HUMANOS + CIBERSEGURIDAD
EL COMPONENTE HUMANO DENTRO DE LA ESTRATEGIA

HumanOS no reemplaza un framework de ciberseguridad. Su función es convertir el componente humano en una conversación práctica dentro de la gestión de riesgo.



HUMANOS PRINCIPLE

La persona no debe ser la última barrera. Debe ser parte de un sistema que combina personas + procesos + tecnología.

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

HUMANOS MANAGER CHECK

¿ESTÁ TU ORGANIZACIÓN PREPARADA?

GOBERNANZA



- [ ] Existe un responsable de awareness/cultura.
- [ ] El riesgo humano forma parte de la conversación de seguridad.
- [ ] Existe una política clara de reporte.

IDENTIDAD



- [ ] MFA en sistemas críticos.
- [ ] Gestión de privilegios.
- [ ] Revisión periódica de accesos.

PERSONAS



- [ ] Capacitación continua.
- [ ] Simulaciones.
- [ ] Capacitación diferenciada por rol.
- [ ] Canal sencillo de reporte.

PROCESOS



- [ ] Validación independiente para operaciones críticas.
- [ ] Procedimientos ante fraude y suplantación.
- [ ] Protocolo post-click.

DETECCIÓN



- [ ] Monitoreo de eventos.
- [ ] Alertas sobre anomalías.
- [ ] Correlación de señales.

RESPUESTA



- [ ] Playbooks definidos.
- [ ] Escalamiento establecido.
- [ ] Responsables claros.
- [ ] Ejercicios periódicos.

MEJORA



- [ ] Métricas.
- [ ] Análisis de incidentes.
- [ ] Lecciones aprendidas.
- [ ] Actualización de controles.

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

HUMANOS 30 DAY START

DE LA GUÍA A LA ACCIÓN

No necesitas transformar todo en 30 días. Necesitas comenzar con prioridades claras.

SEMANA 01
DIAGNÓSTICA



Identifica:

- Riesgos humanos
- Procesos críticos
- Grupos de usuarios
- Canales de reporte
- Controles existentes

RESULTADO

Mapa inicial de riesgo.

SEMANA 02
ACTUALIZA



Refuerza:

- Protocolos
- MFA
- Reporte
- Comunicación interna
- Capacitación priorizada

RESULTADO

Comportamiento esperado definido.

SEMANA 03
SIMULA



Prueba escenarios controlados:

- Phishing
- Suplantación
- MFA fatigue
- Solicitudes financieras
- Ingeniería social

RESULTADO

Comportamiento observado.

SEMANA 04
MIDE + MEJORA



Revisa:

- Reportes
- Tiempo de respuesta
- Errores
- Reincidencias
- Incidentes

RESULTADO

BACKLOG DE MEJORAS.

AL FINAL DE LOS 30 DÍAS

No necesitas tener todo resuelto. Necesitas saber qué riesgo priorizar, qué comportamiento quieres cambiar y qué capacidad debes fortalecer.

LA PREGUNTA QUE DEBERÍA QUEDAR

No: ¿Mis empleados están capacitados?

Sino: ¿QUÉ TAN PREPARADA ESTÁ MI ORGANIZACIÓN CUANDO UNA AMENAZA LOGRA LLEGAR A UNA PERSONA?

Una estrategia madura no depende de que nadie se equivoque.
Depende de que la organización pueda:

PREVENIR - DETECTAR - RESPONDER - APRENDER

¿QUÉ TAN ACTUALIZADA ESTÁ REALMENTE TU ORGANIZACIÓN?

HUMANOS SECURITY SCORE

[DALE CLIC Y EVALUA TU ORGANIZACION

Obtén tu HUMANOS SECURITY SCORE
y descubre dónde existen oportunidades de mejora.

HumanOS

ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

MES DE LA CIBERSEGURIDAD

siscotec | 30 AÑOS Mirando hacia adelante