HumanOS

ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

GUÍA DE AMENAZAS

AMENAZAS QUE TU EQUIPO DEBE RECONOCER

Las amenazas cambiaron. ¿Tu equipo también?

MES DE LA CIBERSEGURIDAD

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

LAS AMENAZAS CAMBIARON ¿TU EQUIPO TAMBIÉN?

La ciberseguridad ya no depende únicamente de firewalls, antivirus, EDR o controles de acceso. Los atacantes también trabajan sobre algo más difícil de proteger: **la confianza humana.**

- Un correo que parece legítimo.
- Un código QR que lleva a una página falsa
- Una llamada que parece venir el CEO
- Una notificación de MFA que llega repetidamene
- Una solicitud urgente de un proveedor
- Una voz que parece ser la de una persona conocida

El objetivo no siempre es atacar directamente un sistema.
Muchas veces es conseguir que una persona realice una acción que favorezca al atacante.

HumanOS Insight

La pregunta ya no es solamente:
¿Tenemos tecnología suficiente?
También es:
¿Nuestro equipo sabe reconocer una amenaza cuando llega disfrazada de una interacción legítima?

siscotec
30 AÑOS
Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

NO NECESITAS SER EXPERTO EN CIBERSEGURIDAD

Necesitas saber cuándo detenerte.

Ante cualquier solicitud inesperada que implique:

Credenciales – dinero - información sensible – acceso – archivos - cambios de cuentas – transferencias - códigos MFA - instalación de software- modificación de procesos.

1



PAUSA

No actúes inmediatamente
La urgencia es una de las herramientas favoritas de la ingenieria social

2



VERIFICA

Confirma la identidad, la solicitud y el contexto mediante un canal independiente y confiable

3



REPORTA

Si algo no tiene sentido, repórtalo.
Reportar rápido puede reducir el impacto de un error

HumanOS RULE

No actuar inmediatamente también es una medida de seguridad.

siscotec
30 AÑOS
Mirando hacia adelante

01 PHISHING CON IA

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

CUANDO EL ENGAÑO EMPIEZA A PARECER DEMASIADO REAL

¿QUÉ ES?

El phishing busca engañar a una persona para que haga algo que beneficia al atacante: entregar credenciales, abrir un archivo, acceder a un sitio falso o realizar una acción financiera. La IA puede hacer que estos mensajes puedan ser más personalizados, coherentes y convincentes.

Señales de alerta

- Urgencia Inesperada
- Solicitud fuera de procedimiento
- Dominio desconocido o ligeramente diferente
- Solicitud de credenciales
- Cambio repentino de una instrucción
- Archivo inesperado
- Solicitud de información sensible

¿Qué hacer?

- Capacitación contextual y recurrente
- Simulación de phishing
- Protección de correo
- MFA resistente al phishing cuando sea viable
- Controles de autenticación de dominio
- Canal sencillo de reporte
- Medir la dificultad del ataque, no solo los clics

HUMANOS

No preguntes solamente "¿parece real?"
Pregunta: "¿Esta solicitud tiene sentido y puedo verificarla por otro canal?"

siscotec 30 AÑOS Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

VER YA NO SIGNIFICA CREER

¿QUÉ ES?

Un deepfake utiliza técnicas de manipulación o generación digital para crear o modificar imágenes, videos o audio que puede utilizarse para fraude, suplantación e ingeniería social, entre otros usos.

Señales de alerta

- Calidad del video
- Sincronización de labios
- Apariencia facial
- Voz
- Fotografia de perfil

¿Qué hacer?

- Doble validación
- Canales previamente establecidos
- Aprobación independiente
- Procedimientos para operaciones financieras
- Controles de identidad
- Registro de autorizaciones

¿DÓNDE ESTÁ EL RIESGO EMPRESARIAL?



¿Dónde está el riesgo empresarial?
Imagina una videollamada:
“Hola, soy el director financiero. Necesito que autorices esta operación antes de las 16:00.”
La imagen parece correcta.
La voz parece correcta.
La solicitud parece coherente.
Pero la identidad puede estar siendo manipulada.

HUMANOS

La confianza no debe depender de lo que vemos en pantalla.

siscotec
30 AÑOS
Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

SI SUENA COMO TU JEFE, ¿REALMENTE ES TU JEFE?

¿QUÉ ES?

La IA permite generar o modificar voces con un nivel de realismo cada vez mayor.

Señales de alerta

Solicitud inesperada

Urgencia Inusual

Cambio ed procedimiento

Solicitud financiera

Información confidencial

No se puede confirmar por el canal habitual

¿Qué hacer?

Toda instrucción crítica debe verificarse por un seguno canal

Llamada - confirmar por Teams

WhatsApp - Confirmar por correo corporativo

Correo - Llamar a un número previamente registrado

Viedo llamada - Aplicar el procedimiento establecido

¿DÓNDE ESTÁ EL RIESGO EMPRESARIAL?



Llamada:
"Jorge, soy el gerente. Estoy entrando a una reunión. Necesito que hagas la transferencia ahora y después te envío el respaldo."
El tono es correcto.
La voz parece familiar.
La urgencia también parece real.

HUMANOS

Una voz conocida no necesariamente es una identidad verificada

siscotec 30 AÑOS Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

UN CÓDIGO QR TAMBIÉN PUEDE LLEVARTE AL LUGAR EQUIVOCADO.

¿QUÉ ES?

El QR phishing, también conocido como quishing, utiliza códigos QR para dirigir a la víctima hacia sitios fraudulentos, formularios, páginas de autenticación o recursos maliciosos. **PUEDE APARECER EN: Correos · Carteles · Eventos · Facturas · Documentos · Mensajería · Publicidad - Incluso encima de códigos legítimos.**

Señales de alerta

Aparece sin contexto

Solicitar iniciar sesion

Pide información financiera

Solicitar descargar una aplicación

¿Qué hacer?

Exige actuar inmediatamente

Lleva a un dominio desconocido

Después de escanearlo, verifica siempre el destino

¿DÓNDE ESTÁ EL RIESGO EMPRESARIAL?



PARA LA ORGANIZACIÓN, No basta con enseñar: "No escanees QR desconocidos."

También debes:

- educar sobre el destino del enlace;
- utilizar filtros de seguridad;
- proteger las cuentas con MFA;
- controlar dominios similares;
- establecer canales oficiales para accesos;
- enseñar a validar la URL después del escaneo.

HUMANOS

El QR oculta el enlace. No elimina el riesgo.

siscotec 30 AÑOS Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

CUANDO LA SEGURIDAD SE CONVIERTE EN UNA MOLESTIA QUE ALGUIEN TERMINA ACEPTANDO.

¿QUÉ ES?

Un atacante que ya posee credenciales puede provocar repetidas solicitudes de autenticación MFA hasta que el usuario, cansado o confundido, termina aceptando una.



El usuario piensa:
"Seguro alguien está intentando entrar.
Acepto para que deje de aparecer."
Ese puede ser precisamente el objetivo.

Regla crítica
Si no iniciaste el acceso, no apruebes el MFA.

CONTROLES:

MFA resistente al phishing cuando sea viable
Number matching cuando corresponda
Alertas ante múltiples intentos
Políticas de bloqueo
Monitoreo de autenticaciones anómalas
Educación
Procedimiento de Reporte

HUMANOS
Una notificación que no solicitaste es una alerta, no una autorización.

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

EL PHISHING LLEGÓ A TU BOLSILLO.

¿QUÉ ES?

El smishing es phishing realizado mediante mensajes de texto u otras plataformas como llamadas, redes sociales y otros canales.



SEÑALES:

Número desconocido
Link acortado
Urgencia
Solicitud de credenciales
Solicitud de códigos
Supuesta institución financiera
Error o Dominio extraño

¿QUÉ HACER?

No responder.
No utilizar el enlace.
Buscar el sitio oficial o utilizar un contacto previamente conocido.

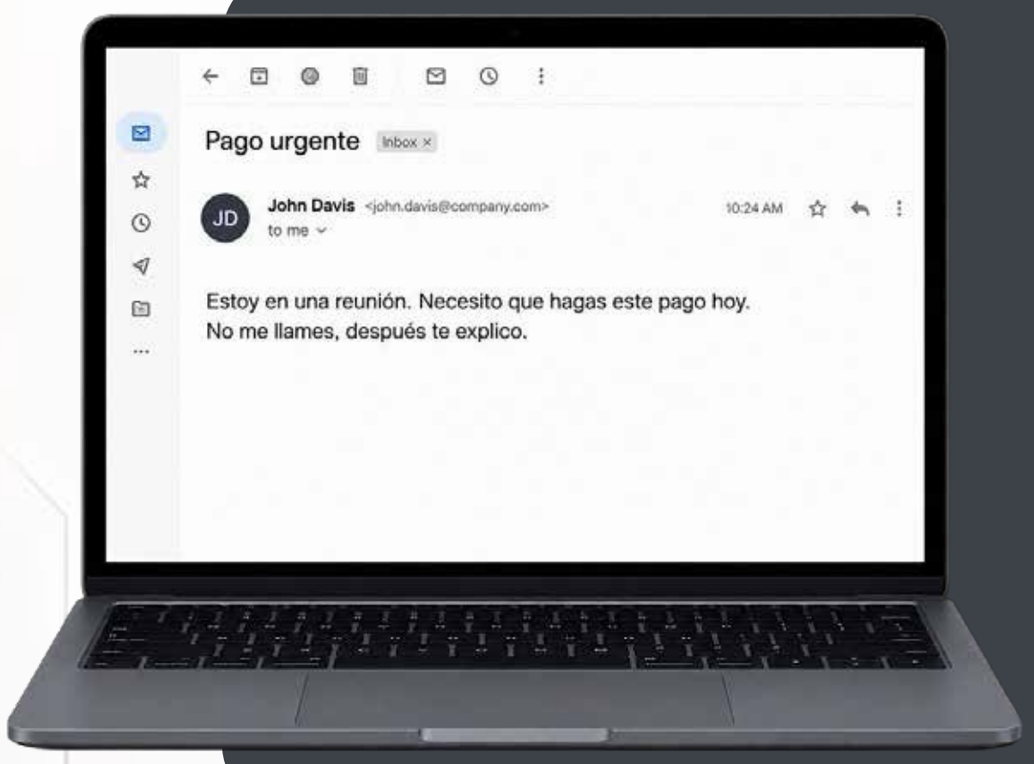
HUMANOS
No porque llegue por WhatsApp o SMS significa que sea confiable.

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

LA AUTORIDAD TAMBIÉN PUEDE SER UTILIZADA COMO ARMA.

¿QUÉ ES?

La suplantación del CEO o de otro ejecutivo utiliza identidad, correo, mensajería o incluso voz para conseguir que un colaborador realice una acción.



El atacante está explotando tres elementos: Autoridad + urgencia + presión

INDICADORES:
"Es confidencial"
"No puedo hablar ahora"
"Hazlo inmediatamente"
Cambio de cuenta bancaria
Cambio de proveedor
Solicitud fuera del procedimiento

CONTROL EMPRESARIAL

Establecer un protocolo para: Pagos + cambios de cuentas + transferencias + información crítica con:

Doble aprobación · Verificación independiente · Contacto previamente registrado · Segregación de funciones · Límites de autorización · Trazabilidad

HUMANOS
La jerarquía nunca debe saltarse el control.

siscotec 30 AÑOS Mirando hacia adelante

08 ROBO DE CREDENCIALES

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

UNA CONTRASEÑA PUEDE SER LA PUERTA DE ENTRADA. LA IDENTIDAD ES EL OBJETIVO.

¿QUÉ BUSCA EL ATACANTE?

No necesariamente entrar directamente a un servidor.

Puede buscar: Usuario · contraseña · token · sesión · cookie · código MFA · correo · credenciales privilegiadas.



¿CÓMO PUEDE OCURRIR?

Phishing
Sitios falsos
Reutilización de contraseñas
Malware
Credential stuffing
Ingeniería social
Robo de sesiones

CONTROLES:

MFA · MFA resistente al phishing cuando sea viable · Contraseñas únicas · Gestores · Gestión de cuentas privilegiadas · Revisión de accesos · Mínimo privilegio · Monitoreo

HUMANOS

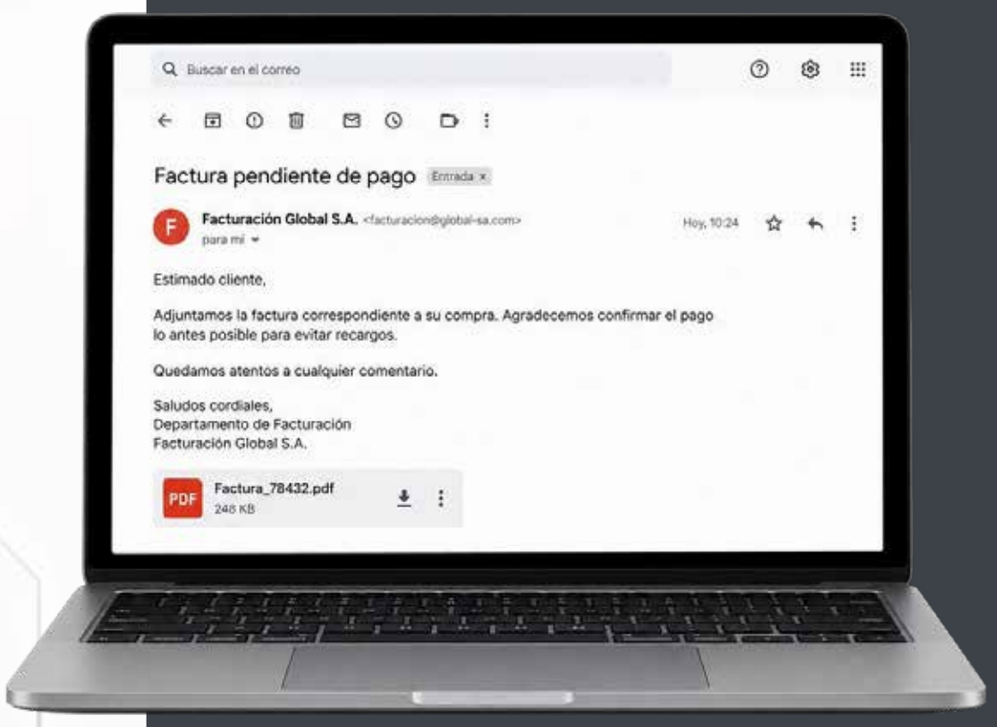
Protege la identidad, no solamente la contraseña

siscotec
30 AÑOS
Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

NO TODO DOCUMENTO ES UN DOCUMENTO.

Un archivo aparentemente legítimo puede utilizarse como mecanismo de entrada para malware. Pueded llegar como:
Factura · Cotización · Orden de compra · Currículum · Contrato · Informe · Documento compartido · Archivo comprimido



SEÑALES

- Archivo inesperado
- Extensión inusual
- Archivo comprimido protegido con contraseña
- Solicitud de habilitar macros o contenido
- Documento enviado desde una cuenta comprometida
- Nombre diseñado para parecerse a otro archivo

CONTROLES:

Secure Email Gateway · EDR/XDR · Sandboxing · Filtrado de extensiones · Bloqueo de archivos de alto riesgo · Actualizaciones y parches · Restricción de macros cuando corresponda · Capacitación de usuarios.

HUMANOS
Protege la identidad, no solamente la contraseña

siscotec
30 AÑOS
Mirando hacia adelante

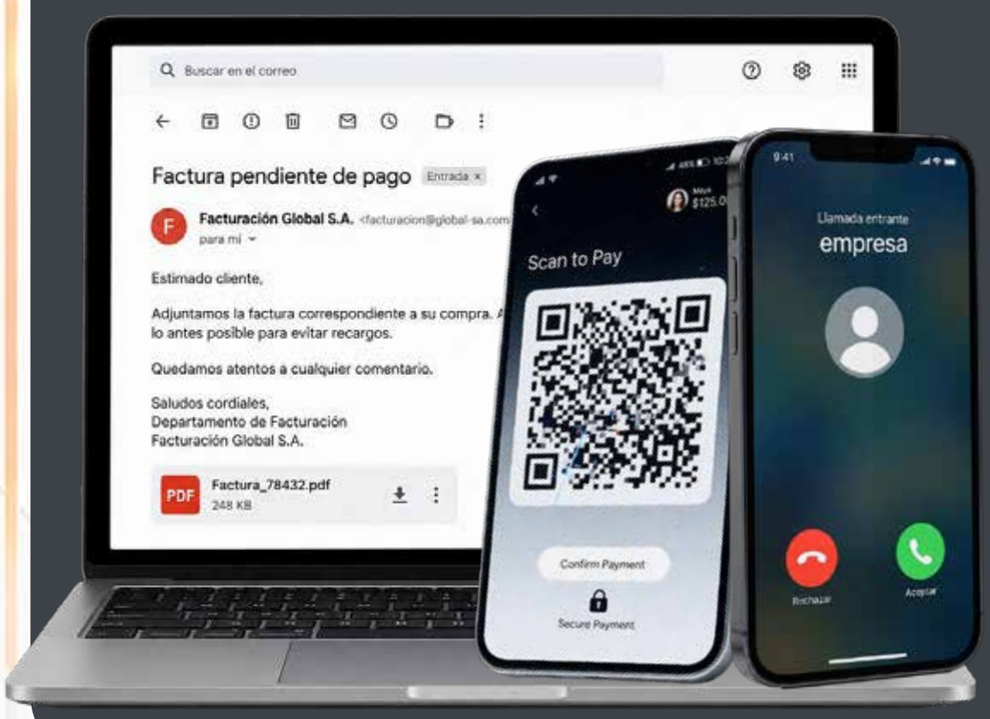
HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

EL ATACANTE NO SIEMPRE NECESITA HACKEAR EL SISTEMA.

A veces intenta convencer a una persona. La ingeniería social explota factores humanos como:

CONFIANZA · AUTORIDAD · URGENCIA · MIEDO · CURIOSIDAD · PRESIÓN · RECIPROCIDAD

UN ATAQUE PUEDE CONSTRUIRSE PASO A PASO



Paso 1: encuentra información sobre un empleado.

Paso 2: identifica a su jefe.

Paso 3: conoce el proveedor con el que trabaja.

Paso 4: envía un correo aparentemente legítimo.

Paso 5: continúa la conversación por WhatsApp.

Paso 6: realiza una llamada.

Paso 7: solicita una acción.

El ataque no depende de un único mensaje. Depende de construir una historia creíble.

PREGUNTAS QUE DEBERÍAN ACTIVAR UNA ALERTA

¿Por qué me lo pide ahora? ¿Por qué debo hacerlo por este canal? ¿Por qué tengo que mantenerlo confidencial? ¿Por qué debo saltarme el procedimiento? ¿Cómo puedo verificar que realmente es esta persona?

CONTROLES EMPRESARIALES

La ingeniería social debe abordarse desde: **Personas + procesos + tecnología**

Una organización debería tener: **Procedimientos claros; Segregación de funciones; Validación independiente; Controles de identidad; Canales de reporte; Simulaciones; Monitoreo; Respuesta ante incidentes.**

HUMANOS

El atacante puede estudiar tu tecnología. También puede estudiar a tu gente.

siscotec
30 AÑOS
Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

EL PATRÓN DETRÁS DE LAS 10 AMENAZAS

NO SON 10 PROBLEMAS AISLADOS.

Muchas de estas amenazas comparten el mismo patron.

01 — GANAR CONFIANZA

Soy tu jefe
Soy tu proveedor

02 — GENERAR PRESIÓN

Es urgente
Ahora

03 — PROVOCAR UNA ACCIÓN

Haz clic
Aprueba
Transfiere
Comparte

04 — OBTENER ALGO

Credenciales
Dinero
Información
Acceso

05 — ESCALAR

Usar ese acceso para continuar el ataque

HUMANOS FRAMEWORK

EL ATAQUE	*LA DEFENSA*
Confía - Presiona - Actúa - Compromete	*Pausa - Verifica - Reporta*

siscotec 30 AÑOS Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

¿QUÉ DEBERÍA HACER UN EQUIPO ACTUALIZADO?

HumanOS no busca que las personas sepan todo.
Busca que sepan cuándo detenerse.



siscotec
30 AÑOS
Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

CHECKLIST PARA CISO / IT MANAGER

¿QUÉ DEBERÍA PODER RESPONDER UN CISO O IT MANAGER?

Una revisión rápida para saber si personas, procesos y tecnología están alineados.

IDENTIDAD	☐ MFA en sistemas críticos. ☐ Privilegios revisados. ☐ Mínimo privilegio. ☐ Métodos resistentes al phishing cuando sea viable.
PERSONAS	☐ Reconocen phishing, smishing y vishing. ☐ Conocen MFA fatigue, deepfakes y clonación de voz. ☐ Saben dónde reportar.
PROCESOS	☐ Pagos y cambios de cuenta con validación independiente. ☐ Procedimientos para solicitudes urgentes. ☐ Excepciones registradas.
TECNOLOGÍA	☐ Protección de correo. ☐ EDR/XDR donde corresponde. ☐ Monitoreo de accesos anómalos. ☐ Parches y actualizaciones.
RESPUESTA	☐ Qué hacer después de un clic. ☐ Canal de escalamiento. ☐ Ejercicios o simulaciones.

DE LA CONCIENCIA A LA RESILIENCIA

SI TU EQUIPO NO SABE QUÉ HACER DESPUÉS DE UN CLIC...

El objetivo no es eliminar el error humano.
Es reducir la probabilidad de que un error se convierta en una brecha.

Si una persona:
hizo clic - detectó - reportó - escaló
la organización tuvo una oportunidad de contener el incidente.
Por eso, además de prevenir, hay que preparar la respuesta.

IDEA CLAVE

La ciberseguridad no termina cuando alguien detecta el problema. También importa qué tan rápido la organización puede detectarlo, responder y recuperarse.

siscotec 30 AÑOS Mirando hacia adelante

¿QUÉ TAN ACTUALIZADO ESTÁ REALMENTE TU EQUIPO?

Reconocer las amenazas es el primer paso. El siguiente es conocer qué tan preparado está tu equipo para enfrentarlas

HUMANOS SECURITY CHECK

HAZ CLIC Y EVALUA TU HUMANOS

Evalúa aspectos relacionados con: Identidad · Personas · Dispositivos Procesos · Detección · Respuesta

Obtén gratis tu HumanOS Security Score

HumanOS

ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

MES DE LA CIBERSEGURIDAD

siscotec

30 AÑOS

Mirando hacia adelante