HumanOS

ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

*SECURITY CHECKLIST*

# ¿QUÉ TAN ACTUALIZADO ESTÁ TU EQUIPO?



**Checklist ejecutivo de 15 minutos**
para identificar hábitos, controles y brechas de visibilidad que conviene reforzar.

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

# EL RIESGO NO SIEMPRE ESTÁ DONDE LO BUSCAMOS

**57%** De las brechas analizadas en Latinoamérica y el Caribe involucraron **el elemento humano.**

Verizon · 2026 Data Breach Investigations Report

En el mismo análisis regional, el phishing representó
**20% de los vectores iniciales de acceso**
y hubo participación de terceros en **74% de las brechas.**

# ¿QUÉ SIGNIFICA?

***La tecnología sigue siendo fundamental.***

Pero una estrategia de ciberseguridad también debe considerar:



**PERSONAS**
**Hábitos, conocimiento y capacidad de detectar amenazas.**



**IDENTIDADES**
**Accesos, privilegios y autenticación.**



**DISPOSITIVOS**
**Visibilidad, actualización y protección.**



**PROCESOS**
**Verificación, reporte y respuesta.**

**HUMANOS UPDATE**

***Tu superficie de ataque no termina en el firewall.***
También incluye a las personas, sus identidades, sus dispositivos y las decisiones que toman todos los días.

siscotec 30 AÑOS Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

# 15 MINUTOS. 24 PREGUNTAS.
# UNA MEJOR VISIÓN

**Este checklist no busca determinar si una organización está "segura" o "insegura".** Su objetivo es ayudarte a identificar qué está implementado, qué necesita atención y dónde existe falta de visibilidad.

| | |
|---|---|
| ✓ | IMPLEMENTADO<br>Existe, está definido y puedes evidenciarlo. |
| ◐ | PARCIAL<br>Existe, pero no está completamente implementado, cubierto o controlado. |
| ✗ | NO IMPLEMENTADO<br>Actualmente no existe o no está formalizado. |
| ? | NO SÉ<br>No tienes suficiente información para responder. |

## HUMANOS INSIGHT

***"No sé" también es un hallazgo.***

Si no puedes determinar quién tiene privilegios administrativos, qué dispositivos están actualizados, si las cuentas críticas tienen MFA o cómo se reporta un incidente, existe una brecha de visibilidad que merece atención.

## ANTES DE EMPEZAR

***No respondas según lo que debería ocurrir.***

Responde según lo que realmente puedes demostrar.

siscotec 30 AÑOS Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

# ¿QUIÉN PUEDE ACCEDER A QUÉ Y CÓMO SABEMOS QUE REALMENTE ES QUIEN DICE SER?

| CHECK | ¿QUÉ DEBERÍAS PODER EVIDENCIAR? | ESTADO |
|---|---|---|
| **MFA en cuentas críticas** | MFA habilitada en correo, VPN, aplicaciones críticas y cuentas privilegiadas. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Revisión periódica de accesos** | Los accesos se revisan ante altas, bajas, cambios de rol y accesos privilegiados. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Privilegios limitados** | Cada usuario tiene únicamente los permisos necesarios para su función. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Autenticación resistente al phishing** | Se evalúan mecanismos resistentes al phishing para cuentas y escenarios de alto impacto, cuando son viables. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |

## ¿POR QUÉ IMPORTA?

La gestión de identidad, autenticación y control de acceso forman parte de las capacidades de protección contempladas por NIST CSF 2.0. CISA también recomienda habilitar MFA en las cuentas que la ofrecen.

**HUMANOS UPDATE**

*Una contraseña no debería ser la única barrera entre una identidad y un activo crítico.*

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

# ¿QUÉ PASA SI UNA CREDENCIAL ES COMPROMETIDA O UN DISPOSITIVO QUEDA SIN ACTUALIZAR?

## CREDENCIALES

| CHECK | ¿QUÉ DEBERÍAS PODER EVIDENCIAR? | ESTADO |
|---|---|---|
| **Credenciales únicas** | No existe reutilización de contraseñas entre servicios críticos. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Gestor de contraseñas** | Existe una herramienta aprobada y una política clara de uso cuando corresponde. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Passkeys** | Se evalúa el uso de passkeys en servicios compatibles y de alto valor. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Cuentas privilegiadas** | Las credenciales administrativas tienen controles y gestión diferenciados. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |

## DISPOSITIVOS Y ACTUALIZACIONES

| CHECK | ¿QUÉ DEBERÍAS PODER EVIDENCIAR? | ESTADO |
|---|---|---|
| **Sistemas operativos actualizados** | Existe política de parcheo y puedes medir su cumplimiento. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Aplicaciones críticas actualizadas** | Existe inventario y se conocen versiones soportadas. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Actualizaciones automáticas** | Están habilitadas cuando son viables y las excepciones están documentadas. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Endpoints bajo control** | Los dispositivos cuentan con protección, configuración, cifrado y gestión definidos. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |

**HUMANOS UPDATE**

*Un dispositivo que no puedes ver, gestionar o actualizar también representa una zona de incertidumbre.*

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

# ¿TU EQUIPO SABE CUÁNDO DEBE DETENERSE?

| CHECK | ¿QUÉ DEBERÍAS PODER EVIDENCIAR? | ESTADO |
|---|---|---|
| **Reconocimiento de señales** | El equipo identifica urgencia, solicitudes inusuales, remitentes, enlaces o archivos sospechosos. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Más allá del email** | La capacitación contempla SMS, llamadas, mensajería, redes sociales y otros canales. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Verificación de solicitudes sensibles** | Dinero, datos, credenciales y cambios de cuenta requieren verificación independiente. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Entrenamiento periódico** | Existen actividades de formación y ejercicios adaptados al contexto de la organización. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Reporte de incidentes** | Los colaboradores conocen un canal claro y sencillo para reportar situaciones sospechosas. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |

**HUMANOS RULE**

Si genera urgencia, involucra dinero, datos o credenciales:

***DETENTE. VERIFICA. REPORTA.***

El phishing puede llegar por múltiples canales y NIST recomienda que las organizaciones preparen a sus colaboradores para reconocer y reportar este tipo de amenazas.

**HUMANOS INSIGHT**

***No se trata solamente de evitar que alguien haga clic.***
Se trata de desarrollar la capacidad de detenerse, cuestionar, verificar y reportar.

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

# ¿TU EQUIPO SIGUE CONFIANDO EN LO QUE VE O ESCUCHA SIN VERIFICAR?

**La inteligencia artificial está haciendo que algunas técnicas de ingeniería social sean más convincentes.** Por eso, las organizaciones necesitan reforzar un principio básico:

## LA IDENTIDAD DEBE VERIFICARSE.

| CHECK | ¿QUÉ DEBERÍAS PODER EVIDENCIAR? | ESTADO |
|---|---|---|
| **Riesgo de suplantación conocido** | El equipo conoce los riesgos de suplantación mediante IA. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Verificación independiente** | Las solicitudes de alto impacto requieren una segunda vía de verificación. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Voz, imagen o video no son prueba suficiente** | Una identidad no se valida únicamente por contenido audiovisual. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Procedimiento para solicitudes inusuales** | Existen reglas para validar solicitudes extraordinarias de ejecutivos, proveedores o terceros. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |

## SOLICITUDES QUE DEBEN VERIFICARSE

*"Necesito que transfieras este dinero ahora."*

*Envíame las credenciales de acceso.*

*No puedo hablar por teléfono, hazlo inmediatamente*

*Soy el gerente. Cambia la cuenta del proveedor.*

### HUMANOS UPDATE

***La IA puede hacer que un engaño parezca real.***
***La verificación sigue siendo humana.***

CISA advierte que la IA puede facilitar la suplantación de personas mediante contenido sintético y recomienda mantener prácticas fundamentales como MFA, contraseñas seguras, actualizaciones y prevención/reportes de phishing.

siscotec 30 AÑOS Mirando hacia adelante

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

# ¿QUÉ OCURRE DESPUÉS DE QUE ALGUIEN DETECTA ALGO SOSPECHOSO?

| CHECK | ¿QUÉ DEBERÍAS PODER EVIDENCIAR? | ESTADO |
|---|---|---|
| **Canal de reporte** | Existe un canal claro, conocido y accesible para reportar incidentes. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Usuarios preparados** | Los colaboradores saben cuándo y cómo utilizarlo. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Responsable definido** | Existe un responsable para recibir, analizar y escalar alertas. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Procedimientos de respuesta** | Existen procedimientos definidos para contener, escalar y responder ante incidentes. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Aprendizaje posterior** | Los incidentes y casi-incidentes generan acciones de mejora. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |
| **Detección y monitoreo** | Existe capacidad técnica para detectar y analizar actividades sospechosas. | ☐ Implementado ☐ Parcial ☐ No implementado ☐ No sé |

## HUMANOS INSIGHT

***DETECTAR ES IMPORTANTE.***
***Saber qué hacer después es capacidad de defensa.***

La gestión de incidentes en NIST CSF 2.0 contempla preparación, análisis, respuesta, comunicación, mitigación y recuperación.

## PREGUNTA PARA EL EQUIPO DE TI

Si mañana un colaborador reporta un correo sospechoso,
***¿quién recibe la alerta, quién decide qué hacer y cuánto tiempo pasa hasta que se analiza?***

**REPORTAR, DETECTAR Y RESPONDER**

HumanOS
ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

## TU HUMANOS SECURITY SNAPSHOT

# AHORA, MIRA TU CHECKLIST COMO UN TODO.

No necesitas convertir esta revisión en un número artificial. Busca patrones.



### HUMANOS ACTUALIZADO

La mayoría de los controles revisados están implementados y existe evidencia para demostrarlo.
***Siguiente paso: mantener, medir y revisar periódicamente.***



### HUMANOS EN ACTUALIZACIÓN

Existen controles parciales, excepciones o áreas donde la evidencia es insuficiente.
***Siguiente paso: identificar las 3 prioridades que deberían abordarse primero.***



### HUMANOS NECESITA ATENCIÓN

Existen controles críticos no implementados o áreas relevantes donde existe poca o ninguna visibilidad.
***Siguiente paso: elevar la revisión, definir responsables y establecer un plan de acción.***

## LAS 3 PREGUNTAS QUE DEBERÍAS PODER RESPONDER

***¿QUÉ NO ESTÁ IMPLEMENTADO?***
***¿QUÉ NO PUEDO EVIDENCIAR?***
***¿QUÉ NECESITO PRIORIZAR?***

siscotec 30 AÑOS Mirando hacia adelante

# ¿QUÉ TAN PREPARADO ESTÁ REALMENTE TU EQUIPO?

**Este checklist es una primera fotografía, no una auditoría ni una evaluación integral de ciberseguridad.** La exposición real depende del contexto de la organización, sus activos, identidades, amenazas, controles, procesos y capacidad de detectar, responder y recuperarse.

# ¿QUIERES SABER QUÉ TAN PREPARADO ESTÁ TU HUMANOS?

Lleva esta revisión un paso más allá. Realiza el HumanOS Security Check, nuestra evaluación digital. Haz clic en el siguiente enlace y realiza el test:

## HACER EL TEST

Al finalizar podrás conocer tus principales áreas de atención y qué aspectos deberías priorizar.

HumanOS

ACTUALIZA EL EQUIPO. PROTEGE EL NEGOCIO

**MES DE LA CIBERSEGURIDAD**

siscotec

30 AÑOS

Mirando hacia adelante