ÓKTARITECH

Human-Centric Cybersecurity Leadership

INSIGHT BRIEF™

EDICIÓN 03

CUANDO PROTEGERSE TAMBIÉN CANSA

Fatiga de seguridad en colaboradores

Más controles no siempre producen mejores decisiones.

Cuando la seguridad interrumpe, confunde o agota, las personas comienzan a ignorarla.

ENFOQUE HUMANO | DECISIONES INTELIGENTES | IMPACTO REAL

ÓKTARITECH
Human-Centric Cybersecurity Leadership
INSIGHT BRIEF™
EDICIÓN 03

LA SEGURIDAD TAMBIÉN PUEDE CONVERTIRSE EN FRICCIÓN

Durante años, las organizaciones han incorporado más contraseñas, alertas, verificaciones, capacitaciones, políticas, bloqueos y procesos de aprobación.

Cada medida puede tener una justificación válida.

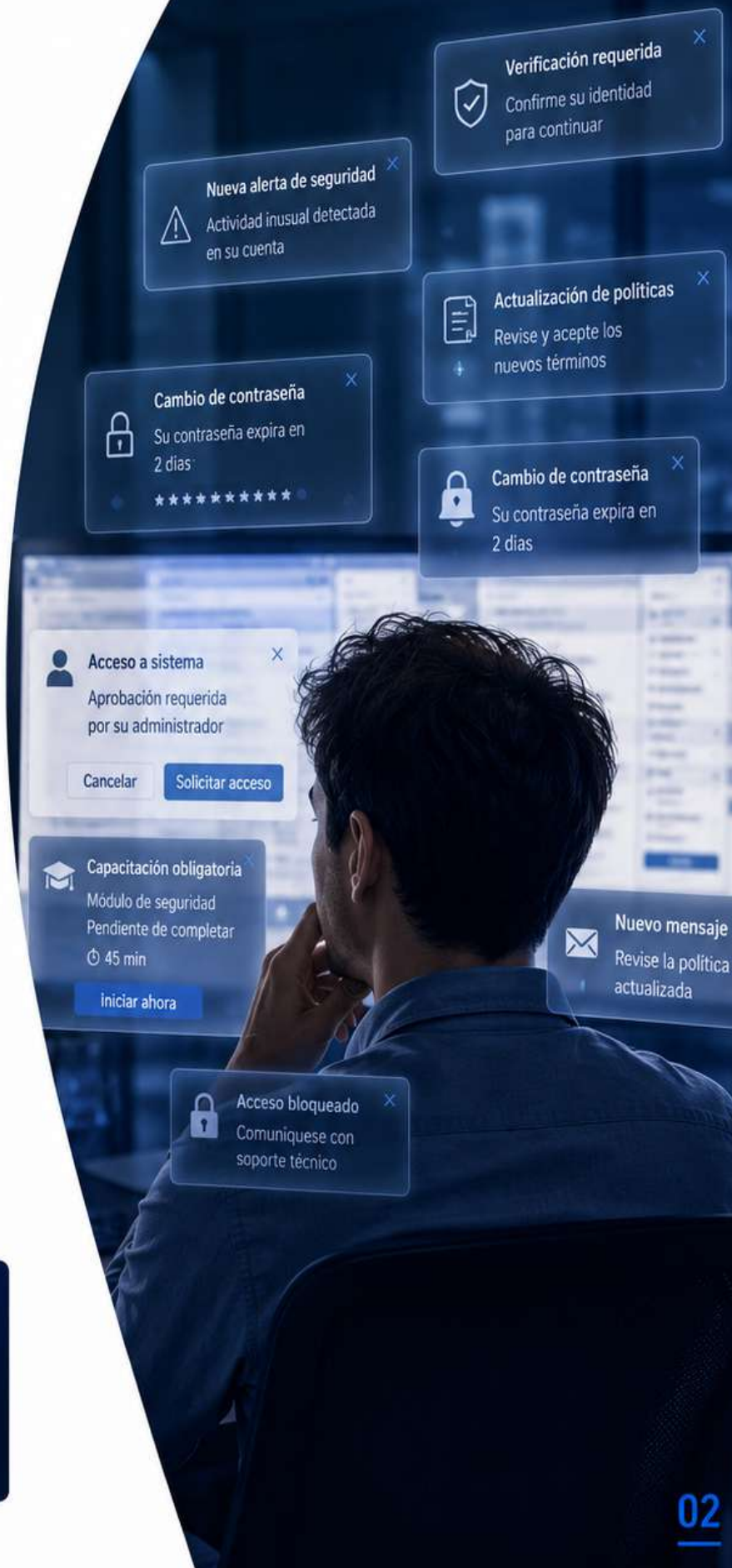
El problema aparece cuando todas compiten simultáneamente por la atención del colaborador.

Cuando protegerse exige detenerse constantemente, recordar demasiadas reglas o interpretar advertencias poco claras, la seguridad comienza a sentirse como una carga adicional al trabajo.

La fatiga no significa que las personas hayan dejado de valorar la seguridad.

Significa que el modelo utilizado para involucrarlas está consumiendo más atención de la que pueden sostener.

> Una organización puede tener controles correctos y, al mismo tiempo, una experiencia de seguridad **insostenible.**



ÓKTARITECH
Human-Centric Cybersecurity Leadership
INSIGHT BRIEF™
EDICIÓN 03

¿QUÉ ES LA FATIGA DE SEGURIDAD?

Es la pérdida progresiva de atención, disposición o capacidad de respuesta que puede aparecer cuando una persona enfrenta **demasiadas decisiones, interrupciones o exigencias** relacionadas con la seguridad.

Puede manifestarse cuando el colaborador:

- recibe demasiadas alertas;
- debe completar verificaciones repetitivas;
- encuentra políticas difíciles de comprender;
- participa constantemente en capacitaciones similares;
- debe memorizar numerosas reglas;
- percibe que cada acción cotidiana requiere una excepción;
- no comprende cuáles advertencias son realmente prioritarias.

NO SIEMPRE SE VE COMO CANSANCIO

También puede expresarse como:

AUTOMATISMO
Aceptar una solicitud sin leerla.

RESIGNACIÓN
Pensar que cumplir correctamente es demasiado difícil.

EVASIÓN
Buscar formas de evitar un control.

NORMALIZACIÓN
Ignorar advertencias porque aparecen constantemente.

DEPENDENCIA
Trasladar cualquier decisión al área de tecnología.

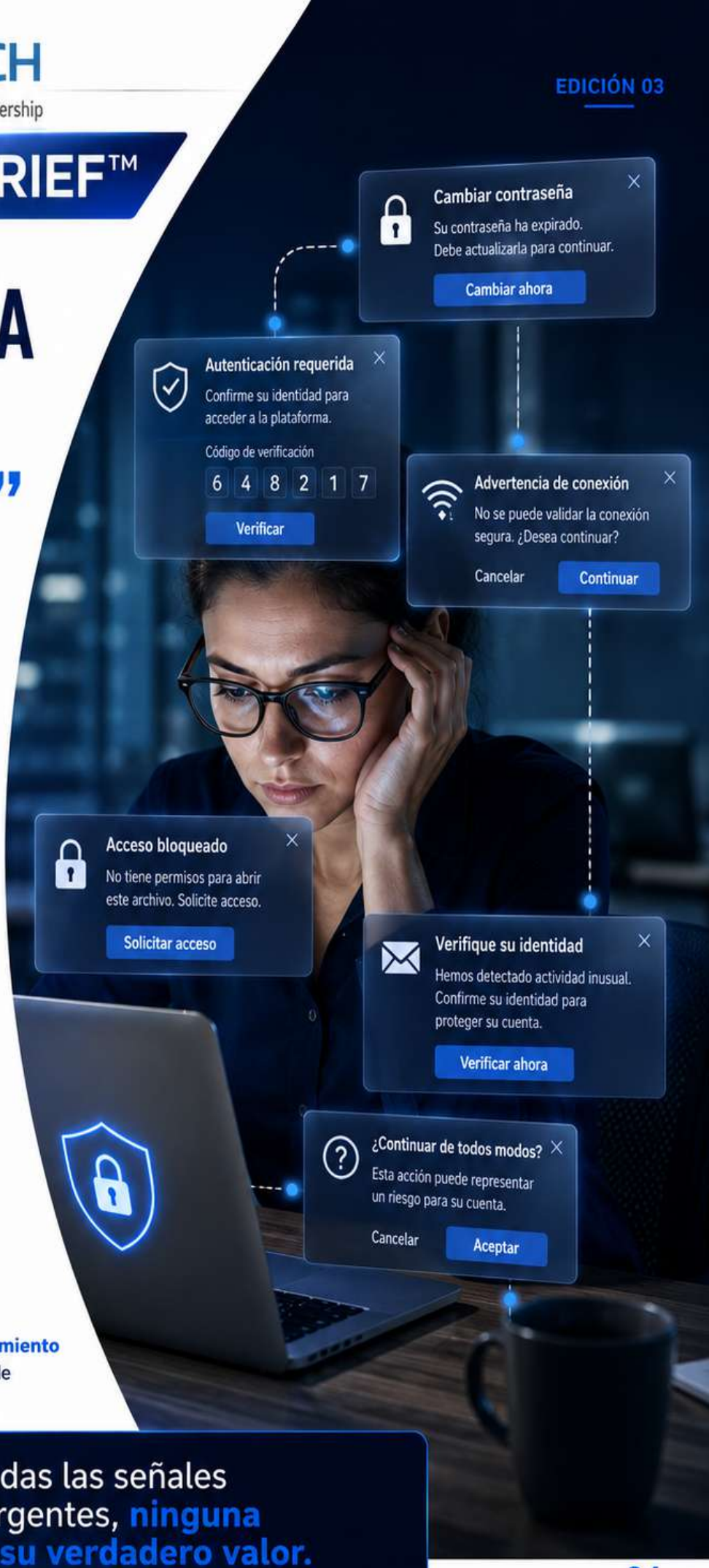
ÓKTARITECH
Human-Centric Cybersecurity Leadership
INSIGHT BRIEF™
EDICIÓN 03

"SOLO QUERÍA TERMINAR EL TRABAJO"

1. Una colaboradora intenta ingresar a una plataforma para completar un proceso urgente.
2. Primero debe cambiar su contraseña.
3. Después recibe una solicitud de autenticación.
4. Luego aparece una advertencia de conexión.
5. Más tarde, el sistema bloquea el archivo que necesita abrir.
6. Finalmente, recibe un correo que le solicita verificar nuevamente su identidad.

En algún momento deja de evaluar cada mensaje. Solo comienza a presionar **Aceptar**.

No actuó con intención de exponer a la empresa. Actuó desde **el agotamiento** generado por un proceso que dejó de ayudarla a distinguir lo importante.



> Cuando todas las señales parecen urgentes, **ninguna conserva su verdadero valor.**

INSIGHT BRIEF™

MÁS COMPLEJIDAD. MÁS DECISIONES. MENOS ATENCIÓN DISPONIBLE.

Las organizaciones operan actualmente en un entorno de mayor complejidad digital, regulatoria y tecnológica. El crecimiento de las amenazas, la adopción acelerada de inteligencia artificial, las cadenas de suministro interconectadas y la escasez de talento especializado están incrementando la presión sobre los modelos de ciberseguridad.

El Foro Económico Mundial reportó que **dos de cada tres** organizaciones enfrentaban brechas de habilidades de moderadas a críticas y que **únicamente el 14 %** confiaba en contar con el talento y las capacidades necesarias.

Al mismo tiempo, el factor humano continúa presente en una proporción considerable de las brechas analizadas globalmente. El **DBIR 2025 de Verizon** examinó 22.052 incidentes y 12.195 brechas confirmadas; sus conclusiones mantienen una participación relevante de acciones humanas, ingeniería social y abuso de credenciales.

TENDENCIAS QUE AUMENTAN LA PRESIÓN SOBRE LA SEGURIDAD

- Aumento sostenido de amenazas sofisticadas
- Adopción acelerada de inteligencia artificial
- Cadenas de suministro cada vez más interconectadas
- Escasez global de talento especializado
- Mayor complejidad regulatoria y de cumplimiento

BRECHAS DE HABILIDADES EN CIBERSEGURIDAD
Foro Económico Mundial 2024

organizaciones enfrentaban brechas de habilidades de moderadas a críticas.

14%

confiaba en contar con el talento y las capacidades necesarias.

Fuente: Global Cybersecurity Outlook 2024 – World Economic Forum

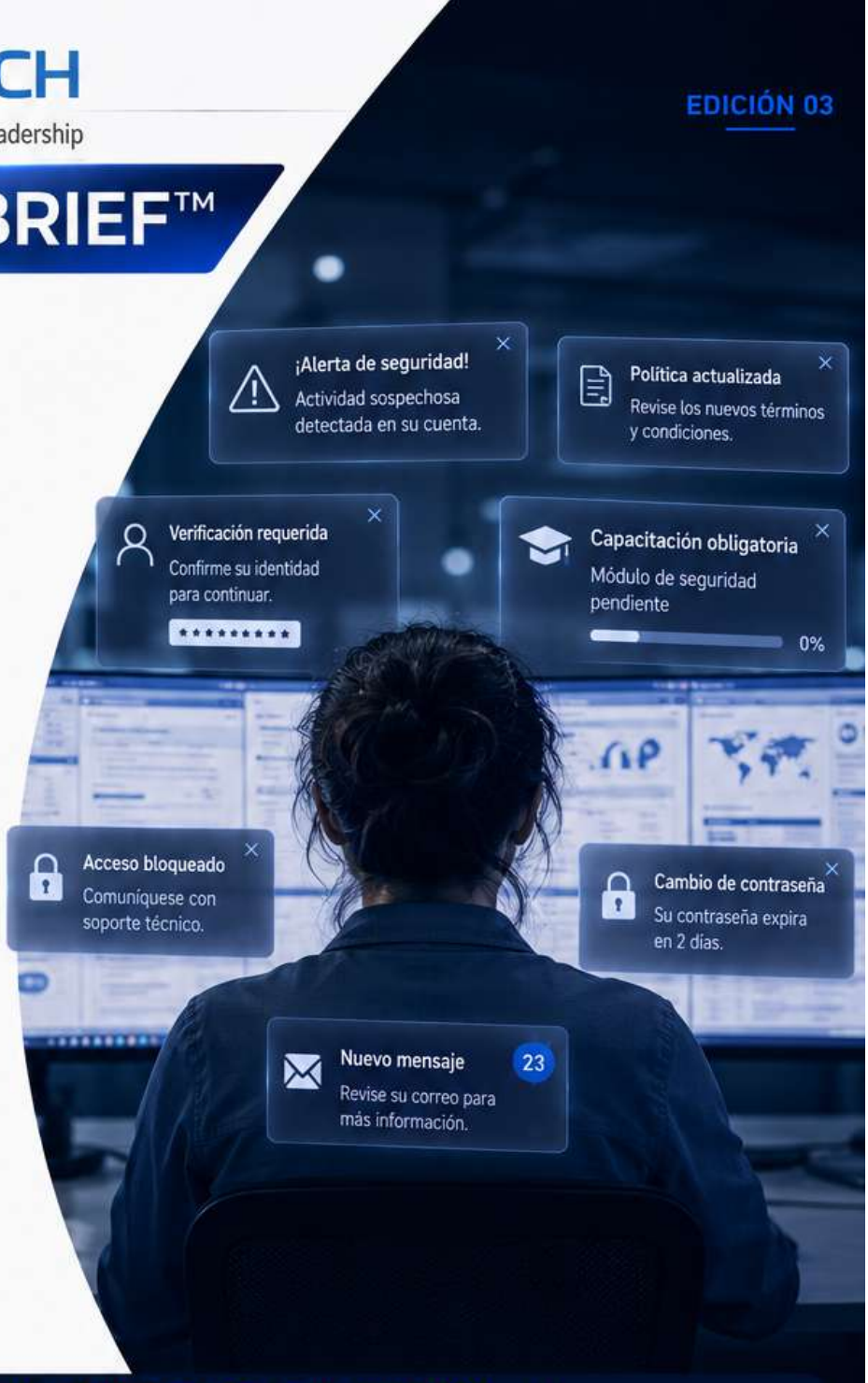
> La complejidad de las amenazas no puede resolverse **trasladando toda la complejidad al colaborador.**

EL DESAFÍO EMERGENTE

La respuesta organizacional suele consistir en agregar:

- Otra alerta
- Otra capacitación
- Otra política
- Otro procedimiento
- Otra validación
- Otro mensaje de advertencia

Pero cada nuevo control también **compite por atención.**



>> LA CARGA INVISIBLE QUE ENFRENTA CADA COLABORADOR >>

80%
de los incidentes involucran el factor humano
Verizon DBIR 2025

56%
de las brechas incluyen el uso indebido de credenciales
Verizon DBIR 2025

2 de 3
organizaciones enfrentan brechas de habilidades de moderadas a críticas
WEF 2024

14%
confía en contar con el talento y capacidades necesarias
WEF 2024

EL CONTEXTO ES CLARO:
El entorno es más complejo, las amenazas más sofisticadas y la presión sobre las personas mayor que nunca.

El verdadero reto no es solo tecnológico, **es humano, operativo y sostenible.**

SE MIDE EL CUMPLIMIENTO. NO SIEMPRE SE MIDE EL AGOTAMIENTO.

Las organizaciones suelen enfocarse en indicadores que demuestran actividad, pero no necesariamente revelan la carga real que enfrentan las personas.

LAS ORGANIZACIONES SUELEN CONOCER:

- Porcentaje de capacitaciones completadas
- Número de simulaciones realizadas
- Cantidad de alertas enviadas
- Aceptación del código de seguridad
- Porcentaje de usuarios con autenticación multifactor
- Número de incidentes reportados

VS.

PERO RARA VEZ CONOCEN:

- Cuántas decisiones de seguridad enfrenta una persona durante su jornada
- Cuántas alertas son ignoradas por repetición
- Qué controles generan mayor fricción operativa
- Cuántas excepciones informales utilizan los equipos
- Qué políticas resultan difíciles de comprender
- Cuánto tiempo exige cumplir con los controles
- Dónde la seguridad compite directamente con los objetivos laborales

> Completar una capacitación no demuestra que **la seguridad pueda sostenerse bajo presión.**

EL PROBLEMA NO SE RESUELVE CON MÁS RECORDATORIOS

Muchas organizaciones están reforzando mensajes sin revisar la experiencia completa.

NO ESTÁN:

- Simplificando controles redundantes.
- Clasificando alertas según su impacto.
- Integrando seguridad en los procesos cotidianos.
- Evaluando la carga cognitiva de los colaboradores.
- Diferenciando formación de información.
- Midiendo la facilidad con la que puede cumplirse una política.
- Revisando si las metas operativas contradicen los controles.
- Involucrando a las personas en el diseño de las medidas.

Cuando una política es difícil de aplicar, la respuesta habitual es **recordar que debe cumplirse.**

La respuesta estratégica debería ser **investigar por qué cumplirla exige tanto esfuerzo.**

PREGUNTAS QUE DEBERÍAN LLEGAR A LA MESA DIRECTIVA

1. ¿Cuántas **interrupciones** de seguridad enfrenta un colaborador durante una jornada normal?
2. ¿Cuáles controles generan más **excepciones, evasiones** o solicitudes de ayuda?
3. ¿Las alertas permiten distinguir claramente entre **información, precaución y urgencia**?
4. ¿Estamos capacitando para **tomar decisiones** o únicamente para completar contenidos?
5. ¿Las políticas están escritas para proteger a la organización o para que las **personas puedan aplicarlas**?
6. ¿Los objetivos de **productividad** incentivan a **omitir algún control**?
7. ¿Qué comportamientos atribuimos a "falta de conciencia" que podrían ser consecuencia de un **diseño deficiente**?
8. ¿Estamos midiendo la **fatiga** antes de que se convierta en **incumplimiento**?

> La pregunta no es únicamente si las personas conocen las reglas. **Es si pueden aplicarlas de forma consistente mientras realizan su trabajo.**

INSIGHT BRIEF™

LA FATIGA NO PERMANECE EN LA PERSONA

Cuando la seguridad consume demasiada atención, el impacto se extiende a toda la organización.

DECISIONES AUTOMÁTICAS
Las advertencias se aceptan sin evaluación.

NORMALIZACIÓN DE ALERTAS
Los mensajes legítimos pierden capacidad de generar respuesta.

USO DE RUTAS ALTERNATIVAS
Las personas buscan herramientas, canales o mecanismos más rápidos.

MENOR REPORTE
Los colaboradores evitan informar dudas para no retrasar procesos.

FRICCIÓN ENTRE ÁREAS
La seguridad comienza a percibirse como una barrera y no como una capacidad de protección.

DEBILITAMIENTO CULTURAL
Cumplir se convierte en una obligación ocasional, no en una práctica integrada.

RIESGO SILENCIOSO
Los controles continúan registrados como activos, aunque su efectividad real esté disminuyendo.

La fatiga de seguridad no solo aumenta el riesgo.
Reduce la capacidad de la organización para detectar, priorizar y responder cuando realmente importa.

LA VISIÓN OKT

La fatiga de seguridad no debe interpretarse como debilidad humana.

Debe interpretarse como una señal de que el diseño organizacional está exigiendo demasiadas decisiones, con demasiada frecuencia y sin suficiente claridad.

Desde la visión de ÓKTARITECH, una cultura de ciberseguridad madura no busca mantener a las personas permanentemente alertas.

Busca construir entornos en los que:

- lo importante sea **fácil de reconocer**;
- lo seguro sea **más sencillo de ejecutar**;
- las decisiones críticas tengan **apoyo**;
- las alertas conserven **significado**;
- los controles **acompañen la operación**;
- la responsabilidad esté **distribuida correctamente**;
- las personas puedan **detenerse sin ser penalizadas.**

> La seguridad sostenible no depende de exigir atención infinita. **Depende de diseñar mejores decisiones.**

MODELO CONCEPTUAL OKT

DE LA SOBRECARGA A LA CLARIDAD

Un enfoque human-céntrico requiere transformar la experiencia de seguridad desde su origen.

CUATRO MOVIMIENTOS PARA DISEÑAR MEJORES DECISIONES

1. REDUCIR
Eliminar controles, comunicaciones y decisiones redundantes.

2. PRIORIZAR
Diferenciar claramente lo informativo, lo preventivo y lo crítico.

3. INTEGRAR
Incorporar seguridad dentro del flujo normal del trabajo.

4. SOSTENER
Diseñar prácticas que puedan mantenerse aun bajo presión operativa.

- Menos fricción.
- Más comprensión.
- Mejores decisiones.

Este recurso podría convertirse en el elemento metodológico distintivo de la edición.

Transformar la experiencia de seguridad es transformar la capacidad de la organización para tomar **mejores decisiones** cada día.

RECOMENDACIONES ESTRATÉGICAS

Acciones clave para reducir la fatiga de seguridad y fortalecer una cultura de decisiones sostenibles.

1. **Elaborar un mapa de fricción de seguridad**
   Identificar dónde los colaboradores encuentran interrupciones, duplicidades, bloqueos o decisiones innecesarias.

2. **Reducir la densidad de alertas**
   Cada advertencia debe tener un propósito, una prioridad y una acción claramente diferenciada.

3. **Diseñar controles proporcionales**
   No todas las actividades requieren el mismo nivel de validación ni la misma carga operativa.

4. **Sustituir capacitación repetitiva por preparación contextual**
   Formar a las personas alrededor de situaciones reales, decisiones concretas y responsabilidades específicas.

5. **Medir comportamientos, no solo participación**
   Evaluar si las personas reconocen señales, detienen procesos, consultan y reportan correctamente.

6. **Revisar incentivos contradictorios**
   Ningún colaborador debería tener que elegir entre cumplir una meta y respetar un control.

7. **Facilitar el reporte temprano**
   Consultar debe ser rápido, seguro y libre de consecuencias negativas.

8. **Incluir la usabilidad en el gobierno de ciberseguridad**
   Todo control relevante debería evaluarse también por su claridad, facilidad de uso y sostenibilidad.

NIST mantiene una línea de investigación de ciberseguridad centrada en las personas que busca considerar sus necesidades, habilidades y limitaciones para ayudarlas a tomar mejores decisiones de seguridad. Este enfoque respalda la idea de que la efectividad de un control también depende de su diseño y usabilidad.

RECOMENDACIONES ESTRATÉGICAS
(CONTINUACIÓN)

Ocho recomendaciones para reducir la fatiga de seguridad y fortalecer la cultura organizacional.

1. **Elaborar un mapa de fricción de seguridad**
   Identificar dónde los colaboradores encuentran interrupciones, duplicidades, bloqueos o decisiones innecesarias.

2. **Reducir la densidad de alertas**
   Cada advertencia debe tener un propósito, una prioridad y una acción claramente diferenciada.

3. **Diseñar controles proporcionales**
   No todas las actividades requieren el mismo nivel de validación ni la misma carga operativa.

4. **Sustituir capacitación repetitiva por preparación contextual**
   Formar a las personas alrededor de situaciones reales, decisiones concretas y responsabilidades especificas.

5. **Medir comportamientos, no solo participación**
   Evaluar si las personas reconocen señales, detienen procesos, consultan y reportan correctamente.

6. **Revisar incentivos contradictorios**
   Ningún colaborador debería tener que elegir entre cumplir una meta y respetar un control.

7. **Facilitar el reporte temprano**
   Consultar debe ser rápido, seguro y libre de consecuencias negativas.

8. **Incluir la usabilidad en el gobierno de ciberseguridad**
   Todo control relevante debería evaluarse también por su claridad, facilidad de uso y sostenibilidad.

DEL DIAGNÓSTICO A LA MEJORA CONTINUA

Transformar la experiencia de seguridad es un ciclo permanente.

BENEFICIOS ORGANIZACIONALES

- Mayor efectividad de los controles
- Menos fricción, más productividad
- Personas más seguras y empoderadas
- Decisiones más rápidas y confiables
- Cultura de seguridad sostenible

La clave no es exigir más atención.
La clave es diseñar experiencias de seguridad que las personas puedan sostener cada día.

REFLEXIÓN FINAL

PROTEGER NO DEBERÍA SIGNIFICAR AGOTAR

Las personas no llegan a una organización para convertirse en especialistas en cada amenaza, interpretar cada alerta o recordar cada excepción.

Llegan para desempeñar una función.

La responsabilidad de la organización consiste en construir un entorno donde realizar esa función de manera segura sea comprensible, posible y sostenible.

Cuando la seguridad depende de una atención permanente, tarde o temprano **la atención disminuye.**

Cuando depende de decisiones claras, procesos coherentes y controles bien integrados, puede convertirse en **parte natural de la forma de trabajar.**

> La fatiga no se corrige exigiendo mayor compromiso.
> Se corrige diseñando una seguridad que las personas puedan sostener.

ÓKTARITECH

Human-Centric Cybersecurity Leadership

INSIGHT BRIEF™

LA SEGURIDAD QUE PERMANECE NO AGOTA. ORIENTA.

ÓKTARITECH transforma la complejidad de la ciberseguridad en decisiones que las organizaciones pueden comprender, aplicar y sostener.

DECIDE FIRST.
PROTECT BETTER.

oktaritech.com