Unión Internacional de Telecomunicaciones

# UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

# X.1212

(03/2017)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Ciberseguridad

# Consideraciones de diseño para la mejor percepción por el usuario extremo de los indicadores de fiabilidad

Recomendación UIT-T X.1212

UIT-T

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

**REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD**

| | |
|---|---|
| REDES PÚBLICAS DE DATOS | X.1–X.199 |
| INTERCONEXIÓN DE SISTEMAS ABIERTOS | X.200–X.299 |
| INTERFUNCIONAMIENTO ENTRE REDES | X.300–X.399 |
| SISTEMAS DE TRATAMIENTO DE MENSAJES | X.400–X.499 |
| DIRECTORIO | X.500–X.599 |
| GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS | X.600–X.699 |
| GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS | X.700–X.799 |
| SEGURIDAD | X.800–X.849 |
| APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS | X.850–X.899 |
| PROCESAMIENTO DISTRIBUIDO ABIERTO | X.900–X.999 |
| SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES | |
| Aspectos generales de la seguridad | X.1000–X.1029 |
| Seguridad de las redes | X.1030–X.1049 |
| Gestión de la seguridad | X.1050–X.1069 |
| Telebiometría | X.1080–X.1099 |
| APLICACIONES Y SERVICIOS CON SEGURIDAD (1) | |
| Seguridad en la multidifusión | X.1100–X.1109 |
| Seguridad en la red residencial | X.1110–X.1119 |
| Seguridad en las redes móviles | X.1120–X.1139 |
| Seguridad en la web | X.1140–X.1149 |
| Protocolos de seguridad (1) | X.1150–X.1159 |
| Seguridad en las comunicaciones punto a punto | X.1160–X.1169 |
| Seguridad de la identidad en las redes | X.1170–X.1179 |
| Seguridad en la TVIP | X.1180–X.1199 |
| SEGURIDAD EN EL CIBERESPACIO | |
| **Ciberseguridad** | **X.1200–X.1229** |
| Lucha contra el correo basura | X.1230–X.1249 |
| Gestión de identidades | X.1250–X.1279 |
| APLICACIONES Y SERVICIOS CON SEGURIDAD (2) | |
| Comunicaciones de emergencia | X.1300–X.1309 |
| Seguridad en las redes de sensores ubicuos | X.1310–X.1319 |

# Recomendación UIT-T X.1212

## Consideraciones de diseño para la mejor percepción por el usuario extremo de los indicadores de fiabilidad


**Resumen**

Ataques de varios tipos emplean la replicación de contenido de proveedores de servicio fiables, engañando así a los usuarios extremos, que creen en esa falsa fiabilidad.

En la Recomendación UIT-T X.1212 se describen las consideraciones de diseño para la mejor percepción por el usuario extremo de los indicadores de fiabilidad. En los apéndices se describen técnicas representativas para medir la percepción por el usuario extremo de esos indicadores.



**Historia**

| Edición | Recomendación | Aprobación | Comisión de Estudio | ID único* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1212 | 2017-03-30 | 17 | 11.1002/1000/13195 |

**Palabras clave**

Indicadores de fiabilidad, percepción por el usuario extremo, usurpación de identidad.


* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

## PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

## NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

## PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

## ÍNDICE


**Página**

1 Alcance ..... 1
2 Referencias ..... 1
3 Definiciones ..... 1
3.1 Términos definidos en otros documentos ..... 1
3.2 Términos definidos en la presente Recomendación ..... 2
4 Abreviaturas y acrónimos ..... 2
5 Convenios ..... 2
6 Percepción por el usuario extremo de los indicadores de fiabilidad ..... 2
7 Técnicas para mejorar la percepción por el usuario extremo de los indicadores de fiabilidad ..... 2
7.1 Elementos visuales ..... 2
7.2 Elementos narrativos ..... 3
7.3 Transiciones de diseño periférico ..... 4
7.4 Modo de formación ..... 4
7.5 Accesibilidad ..... 4
7.6 Niños ..... 5
Apéndice I – Consideraciones para el análisis de tareas cognitivas para la ciberseguridad ..... 6
I.1 Consideraciones para el análisis de tareas cognitivas para la ciberseguridad ..... 6
I.2 Tres conceptos habilitadores de seguridad de la información ..... 6
I.3 Métodos de medición posibles ..... 6
Apéndice II – Consideraciones sobre la protección de los usuarios extremos mediante el análisis de tareas cognitivas ..... 8
II.1 Estimación de los conocimientos y destrezas del usuario ..... 8
Bibliografía ..... 11

# Recomendación UIT-T X.1212

## Consideraciones de diseño para la mejor percepción por el usuario extremo de los indicadores de fiabilidad

### 1 Alcance

Ataques de diversos tipos utilizan la replicación de contenido de proveedores de servicio fiables, engañando así a los usuarios extremos, que creen en esa falsa fiabilidad. En la presente Recomendación se describen las consideraciones de diseño para la mejor precepción por el usuario extremo de los indicadores de fiabilidad. En los Apéndices se describen técnicas representativas para medir la percepción por el usuario extremo de esos indicadores.

### 2 Referencias

Ninguna.

### 3 Definiciones

#### 3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

**3.1.1 discapacidad** [b-UIT-T F.790]: Se define como un estado en el cual se restringe la utilización de equipos y servicios de telecomunicaciones. En su primera acepción, la "discapacidad" se considera el resultado de una limitación funcional temporal o permanente debida a una enfermedad, un accidente, la vejez, etc. Desde un punto de vista más general, la "discapacidad" corresponde a un estado que hace imposible la plena utilización del equipo y servicios de telecomunicaciones, debido al entorno físico y/o social del caso (por ejemplo, la telefonía vocal en un entorno ruidoso).

**3.1.2 medición** [b-ENISA]: Acción y efecto de medir, que consiste en determinar el valor de una variable cuantitativa respecto de una unidad de medición (normalizada).

**3.1.3 métrica** [b-ENISA]: Sistema de medición relativa que permite la cuantificación de ciertas características del sistema, componente o proceso. La métrica está formada por dos o más mediciones.

**3.1.4 información de identificación personal (PII)** [b-UIT-T X.1252]: Toda información a) que identifica a una persona y que puede utilizarse para identificar, contactar o localizar a la misma; b) que puede utilizarse para obtener información de identificación o de contacto sobre una determinada persona; c) que puede relacionarse directa o directamente con una persona.

**3.1.5 usurpación de identidad (phishing)** [b-UIT X.1254]: Mensaje fraudulento que incita al usuario de correo electrónico a revelar datos personales o confidenciales que el originador del mensaje puede utilizar con fines ilícitos.

**3.1.6 accesibilidad a las telecomunicaciones** [b-UIT-T F.790]: En la esfera de las telecomunicaciones, se trata de la posibilidad de utilización de un producto, servicio o entorno o facilidad por el número más grande posible de usuarios, especialmente, usuarios con discapacidades.

**3.1.7 persona con discapacidad** [b-UIT-T F.791]: El modo correcto de referirse a una persona con discapacidad [b-UNCRPD].

## 3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se define el siguiente término:

**3.2.1 indicadores de fiabilidad**: Símbolos que presenta el agente usuario web para informar a los usuarios extremos de la fiabilidad del sitio web.

# 4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

DKIM Correo identificado mediante la tecnología DomainKeys (*domainkeys identified mail)*

DOM Modelo de objeto de documento (*document object model)*

FNE Miedo a la evaluación negativa (*fear of negative evaluation)*

SSL Capa de zócalo seguro (*secure socket layer)*

URL Localizador de recursos uniforme (*uniform resource locator)*

# 5 Convenios

Ninguno.

# 6 Percepción por el usuario extremo de los indicadores de fiabilidad

Los protocolos para el intercambio de información de ciberseguridad, como se identifican en [b-UIT-T X.1500], pueden transportar información útil para las decisiones de fiabilidad que se tomen en cualquier interacción en el ciberespacio. Entre esa información se incluye, entre otras cosas, la información de certificado de validación ampliada [b-CAB-Baseline], el nivel de garantía de las identidades [b-UIT-T X.1254], las firmas de correo identificado mediante la tecnología DomainKeys (DKIM) del correo-e [b-IETF RFC 6376] y la indicación de los sitios de usurpación de la identidad [b-IETF RFC 5901].

No obstante, con frecuencia los usuarios extremos ignoran o apenas consideran estos indicadores de fiabilidad, según se desprende de estudios anteriores realizados sobre una base demográfica diversa (pueden encontrarse más detalles al respecto en el Apéndice II). Así, es necesario mejorar la percepción por el usuario extremo de los indicadores de fiabilidad.

# 7 Técnicas para mejorar la percepción por el usuario extremo de los indicadores de fiabilidad

En esta cláusula se presentan diversas técnicas para mejorar la percepción por el usuario extremo de los indicadores de fiabilidad. Estas técnicas pueden utilizarse individualmente o combinadas, según se prefiera o sea adecuado, para presentar los indicadores de fiabilidad de manera más reconocible.

## 7.1 Elementos visuales

Los creadores de los indicadores de fiabilidad deberán considerar la posibilidad de emplear elementos visuales normalizados. Estudios anteriores han revelado que los usuarios poco experimentados no están familiarizados con la codificación simbólica de los indicadores de fiabilidad, por ejemplo, en los localizadores de recursos uniformes (URL), y suelen ignorarla [b-Miyamoto]. Por tanto, se recomienda introducir elementos visuales, por ejemplo, iconos que indiquen la fiabilidad. Los implementadores podrán considerar la posibilidad de emplear algunos elementos visuales normalizados, del tipo de la señalética vial, para minimizar la necesidad de aprender y memorizar signos.

De acuerdo con los signos y etiquetas de seguridad de productos [b-ANSI-Z535.4**]**, la utilización de palabras señal (por ejemplo, "Peligro", "Atención") en determinados colores (rojo, naranja, amarillo) reduce el nivel de riesgo.

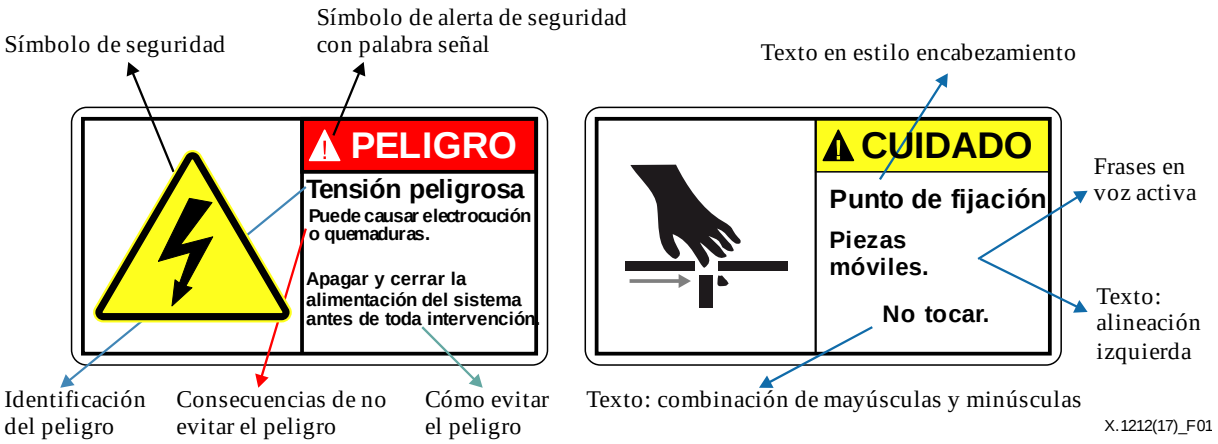



**Figura 1 – Signos y etiquetas de seguridad de productos (ANSI Z535.4)**

El mensaje "PELIGRO" utiliza un triángulo blanco con un signo de exclamación rojo sobre fondo rojo. El mensaje "ATENCIÓN" utiliza un triángulo negro con un signo de exclamación naranja. El mensaje "CUIDADO" emplea un triángulo negro con un signo de exclamación amarillo.

Además, los creadores de indicadores de fiabilidad deben emplear colores normalizados para representar los niveles de fiabilidad. En el contexto de la psicología del color, el rojo se utiliza para atraer la atención. El rojo es la longitud de onda más larga del espectro de la luz visible y tiene la propiedad de aparentar estar más cerca de lo que realmente está. Así, el rojo atrae la atención del usuario y se utiliza para los semáforos. La longitud de onda del amarillo es relativamente larga y básicamente estimulante, por lo que capta la atención del usuario. En el centro del espectro se encuentra el verde, cuya longitud de onda en la luz visible es intermedia. Generalmente el verde no exige un ajuste de la visión, por lo que se utiliza como signo de relajación y tranquilidad. El azul tranquiliza y ayuda a concentrarse.

Los creadores de indicadores de fiabilidad pueden emplear el concepto de "cerebro social", que incita el comportamiento prosocial y cooperativo. Estudios anteriores han determinado que las personas muestran un comportamiento más social cuando tienen cerca imágenes de ojos que miran [b-Rigdon], [b-Senju]. No obstante, hay escépticos que opinan que las imágenes de ojos que miran no influyen en el comportamiento o influyen muy poco [b-Felt2014].

## 7.2 Elementos narrativos

Estudios anteriores han revelado que ciertos grupos de usuarios adoptan decisiones sobre la fiabilidad en función de escritos narrativos, más que de nombres de dominio, tipos de protocolo o URL [b-Felst2014], [b-Felt2015]. Se recomienda equipar el software de usuario extremo con la capacidad de convertir la información simbólica en elementos narrativos sin acrónimos. También puede ser útil para los usuarios con deficiencias visuales, si se combina esa capacidad con sistemas de transformación del texto a voz.

A fin de captar la atención de los usuarios, es decir, en los mensajes de alerta, pueden considerarse diversos criterios de diseño del software de usuario extremo, como los que se indican a continuación:

1) Los creadores de indicadores de fiabilidad deben evitar la utilización de términos técnicos. En los mensajes de alerta, se sustituirán los términos técnicos por frases o expresiones que los usuarios puedan entender, pues ignorarán el mensaje si no saben cómo responder adecuadamente al mismo.

2) Los creadores de indicadores de fiabilidad deben tener en cuenta la brevedad de los mensajes. Una gran cantidad de texto necesitará mucho esfuerzo de lectura, por lo que los usuarios tenderán a ignorarlo. Dentro del mensaje se eliminará el texto redundante a fin de que sea conciso y preciso. Cabe señalar que se ha de llegar a un equilibrio entre la brevedad y la precisión: no es posible explicar todos los aspectos de un modelo de amenaza en un único y breve párrafo. Por consiguiente, las alertas deberán utilizar tanto elementos visuales como textuales. Para calcular el grado de brevedad, los creadores podrán aplicar un índice de legibilidad, que es el patrón de acuerdo con el cual se estima cuántos años de formación académica necesita una persona para entender un texto escrito.

3) Los creadores de indicadores de fiabilidad deben describir el riesgo que se corre o que se va a correr. Los mensajes de alerta deben describir el riesgo subyacente, pues probablemente los usuarios lo entiendan y acaten el mensaje si éste describe explícita e inequívocamente los riesgos. En el mensaje habrán de incluirse además instrucciones para evitar el riesgo, a menos que se desprendan claramente de la exposición del riesgo.

### 7.3 Transiciones de diseño periférico

Los creadores de indicadores de fiabilidad podrán probar su interfaz en relación con las transiciones de diseño periférico. Una transición repentina en el campo de la visión periférica puede ser muy eficaz para señalar un posible riesgo, por lo que se recomienda emplear esta técnica en la transición de diseños periféricos (generalmente denominados, "temas" o "fondos"), siempre que los usuarios extremos se enfrenten a sitios web o mensajes de correo-e de alto riesgo.

### 7.4 Modo de formación

Los creadores de indicadores de fiabilidad pueden preparar modos de formación. La percepción por el usuario extremo del riesgo será, en el mejor de los casos, imprecisa si ese usuario se expone a los riesgos con muy poca frecuencia. Por consiguiente se recomienda dotar al software de usuario extremo con un modo formación en el que se puedan generar artificialmente simulaciones de eventos de riesgo a fin de entrenar la percepción del usuario extremo y mejorar su precisión. Esa formación también puede incentivarse transformándola en un juego.

### 7.5 Accesibilidad

Los creadores de indicadores de fiabilidad deben diseñar su interfaz teniendo en cuenta la accesibilidad. Por visión se entiende la capacidad de distinguir la forma, el tamaño, el volumen y el color de estímulos visuales. Para las personas con deficiencias visuales puede resultar difícil encontrar indicadores de fiabilidad. Debido a efectos conocidos como "protanopia" y "deuteranopia", algunos usuarios extremos tienen dificultades para distinguir los colores, por ejemplo, entre rojo y verde.

La ISO/CEI elabora unas directrices de accesibilidad [b-ISO/CEI-40500] para personas con discapacidad, aunque en esas directrices no se tratan directamente los indicadores de fiabilidad en la barra de dirección. En los requisitos básicos del CA Browser Forum [b-CAB-Baseline] se definen las normas para certificados y autoridades de certificación, aunque no se indica cómo los navegadores deben presentar los certificados a los usuarios.

La lista de verificación de accesibilidad a las telecomunicaciones [b-UIT-T-FSTP-TACL] garantiza que los servicios y funcionalidades especificadas pueden ser accesible por todos los usuarios, incluidas las personas con discapacidad. A fin de ofrecer una mejor accesibilidad para las personas con deficiencias visuales o ceguera, la interfaz debe ofrecer al usuario una presentación de medios, además de poderse controlar de diversos modos y con diversos tipos de acciones de control. Para personas con discapacidad cognitiva, deberán marcarse los puntos importantes para llamar su atención y utilizar medios suplementarios, como iconos, vídeos y audios.

Las aplicaciones de lectura de pantalla pueden extraer los indicadores de fiabilidad de los sitios web. Pueden presentar la información de seguridad, por ejemplo, la barra de dirección verde de un certificado EV-SSL, y leer la información con servicios de transformación de texto a voz. También pueden resumir la información de un árbol de modelo de objeto de documento (DOM) del navegador.

### 7.6 Niños

En lo relativo a los niños que utilizan Internet, los padres suelen comprobar las actividades de sus hijos escuchando u observando lo que comunican o con información que les permite restringir acceso mediante un formato accesible. Esa vía "de protección" puede que no sea accesible para un padre con discapacidad. Esa función concreta se encuentra entre dos esferas: la protección del niño en Internet y la accesibilidad para un padre/adulto con discapacidad y con la responsabilidad de educar a sus hijos con o sin discapacidad.

# Apéndice I

## Consideraciones para el análisis de tareas cognitivas para la ciberseguridad

(Este apéndice no forma parte integrante de la presente Recomendación.)

### I.1 Consideraciones para el análisis de tareas cognitivas para la ciberseguridad

El análisis de tareas cognitivas para la ciberseguridad puede conllevar la medición de elementos del comportamiento, así como el análisis de interacciones, lo que, en último término, lleva a inferir procesos mentales internos. En esta Recomendación se consideran tres conceptos de seguridad de la información, a saber, la confidencialidad, la integridad y la disponibilidad, como requisitos para el análisis de tareas cognitivas para la ciberseguridad.

### I.2 Tres conceptos habilitadores de seguridad de la información

**Confidencialidad**

Entre los datos medidos puede haber información personal, que es fundamentalmente sensible en el plano de la privacidad. Así, esos datos deberán manejarse con cuidado y con el acuerdo previo de los usuarios extremos. Debe controlarse estrictamente la medida en que se comparte tal información.

**Integridad**

Los métodos de medición pueden utilizar la información recopilada independientemente del miedo a la evaluación negativa (FNE). Las observaciones suelen estar afectadas por el FNE, donde algunas personas ocultarán sus errores, ya que hacer públicos los errores suele erosionar el amor propio y menoscabar la reputación profesional.

**Disponibilidad**

Para las observaciones se debe utilizar un método fácilmente aplicable a las personas. En el contexto de la prevención de la usurpación de identidad, los métodos deben estar disponibles mientras los usuarios navegan por la información presentada. Se optará de preferencia por dispositivos sin contacto. Además, los usuarios no llevarán implantes ni otros dispositivos que puedan herirlos de manera alguna.

### I.3 Métodos de medición posibles

La investigación en psicología experimental ha demostrado que existe un fuerte vínculo entre los movimientos oculares y los trastornos mentales [b-Crawford], [b-Noris]. Leigh *et al*. [b-Leigh] clasifican los movimientos oculares en cuatro categorías, a saber, sacádicos, de fijación, de seguimiento y reflejos vestíbulo-oculares. Por norma general, los movimientos oculares sacádicos cambian en función de lo que la persona está viendo. En el contexto del modelo mental, Irwin *et al*. demostraron que la rotación mental se suprime mientras se realiza el movimiento [b-Irwin], y Tokuda [b-Tokuda] demostró que la carga de trabajo mental, el indicador de hasta qué punto una persona está ocupada a nivel mental/cognitivo, puede estimarse a partir de las intrusiones sacádicas.

También pueden realizarse una validación de la temperatura facial superficial para obtener información en forma de medición fisiológica de la condición mental [b-Or], [b-Wang], [b-Volskamp]. En sus experimentos, Genno *et al*. [b-Genno] demostraron que, cuando los sujetos experimentaban sensaciones como el estrés y la fatiga, oscilaba la temperatura en la zona nasal. Por otra parte, combinada con otros métodos de medición, la termografía ofrece un medio flexible y muy automatizado de evaluar objetivamente la carga de trabajo [b-Or].

Paralelamente a lo anterior, para obtener información se suelen medir la actividad cerebral, la conductividad de la piel, las constantes cardiacas y la tensión arterial, aunque son pruebas obstructivas para el usuario. El reconocimiento de las expresiones y gestos faciales es útil en cuanto a la disponibilidad, pero sufre fácilmente la influencia del FNE.

# Apéndice II

## Consideraciones sobre la protección de los usuarios extremos mediante el análisis de tareas cognitivas

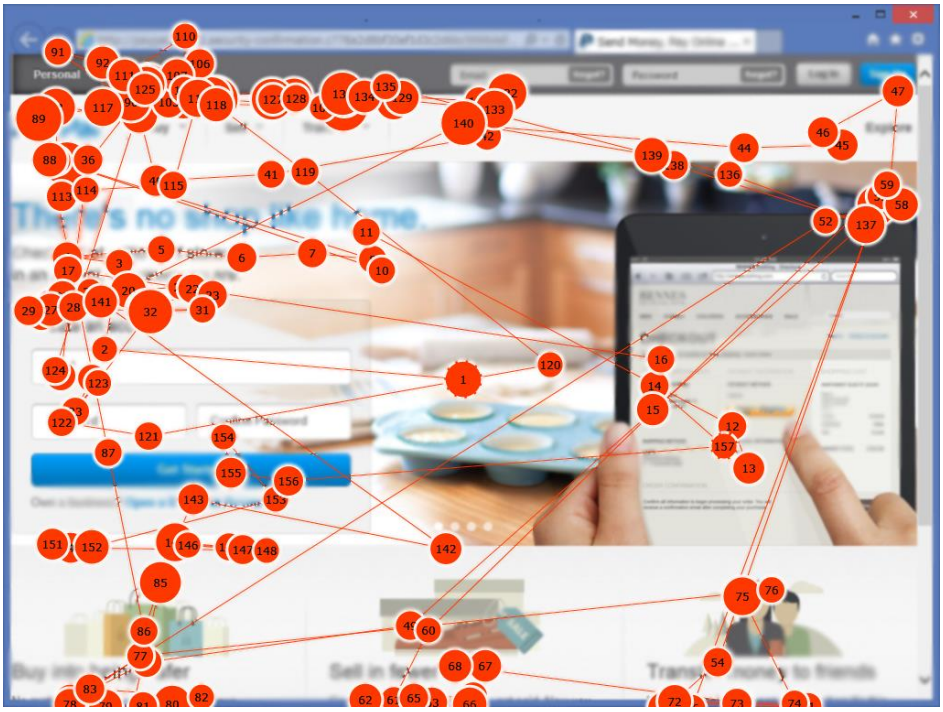
(Este apéndice no forma parte integrante de la presente Recomendación.)

### II.1 Estimación de los conocimientos y destrezas del usuario

De un estudio anterior se desprende que los usuarios extremos pueden categorizarse en dos tipos: expertos e inexpertos [b-Miyamoto]. Los expertos evalúan el URL de un sitio y/o el indicador de la capa de zócalo seguro (SSL) en lugar de los contenidos de la página para juzgar la credibilidad del sitio. Por el contrario, los inexpertos se ven más influidos por los contenidos web. Por su misma naturaleza, los contenidos web de los sitios de usurpación de la identidad son muy similares a los de los sitios legítimos, lo que hace que los inexpertos caigan en la trampa.

Esa característica diferenciadora de los usuarios extremos resulta útil para personalizar la prevención contra la usurpación de la identidad. Una posibilidad consiste en ofrecer ejercicios de detección de usurpación de identidad con una baja tasa de falsos negativos para los inexpertos y de falsos positivos para los expertos. Por lo general, los sistemas de prevención contra la usurpación de la identidad tienen problemas de precisión de detección, porque se ha de llegar a un equilibrio entre los falsos positivos (sitios legítimos etiquetados como falsos) y los falsos negativos (sitios de usurpación etiquetados como legítimos). Los falsos positivos aumentarán si el sistema se centra en reducir los falsos negativos (sitios de usurpación etiquetados como legítimos). Se considera difícil reducir los dos errores. Alternativamente, el sistema debe proteger a los inexpertos, que suelen tomar la decisión incorrecta.

Los dispositivos de seguimiento de la mirada facilitan la identificación de los usuarios web inexpertos. En la Figura II.1 se muestra el movimiento ocular de un inexperto ante un sitio web de usurpación de la identidad. En la Figura II.2 se muestra el movimiento ocular de un usuario experto. Los círculos marcan las fijaciones y el número dentro de ellos indica su orden. En el caso de la usurpación de la identidad, el inexperto mira el contenido de la página, pero ignora la barra de dirección del navegador al evaluar la credibilidad, como se ve en la Figura II.1.



X.1212(17)_FII.1

**Figura II.1 – Usuario inexperto en un sitio web de usurpación de la identidad**

X.1212(17)_FII.2

**Figura II.2 – Usuario experto en un sitio de usurpación de la identidad**

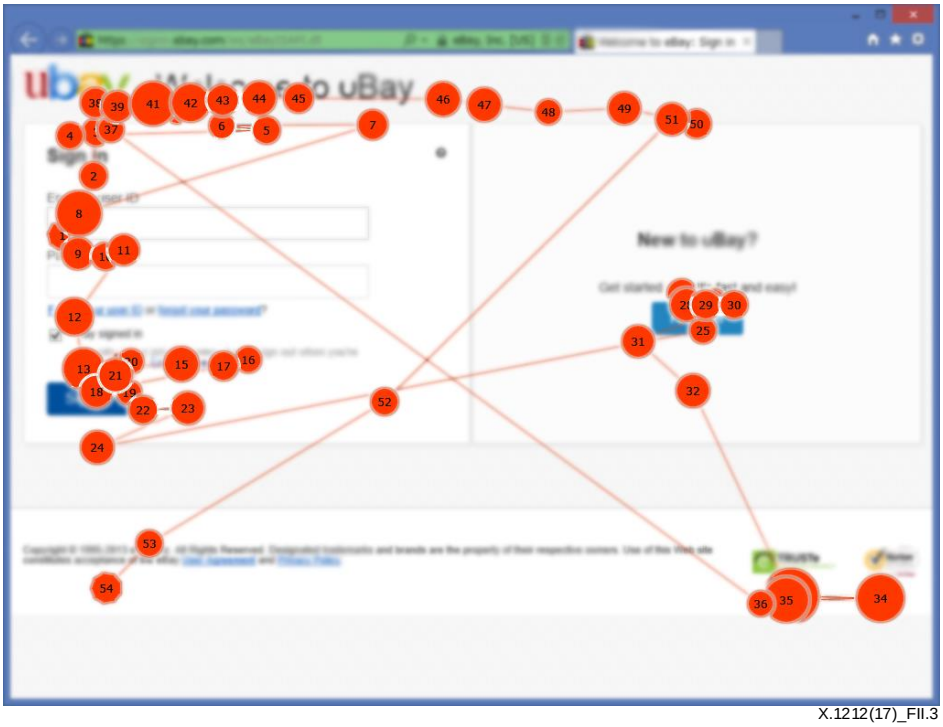



**Figura II.3 – Usuario inexperto en un sitio web legítimo**

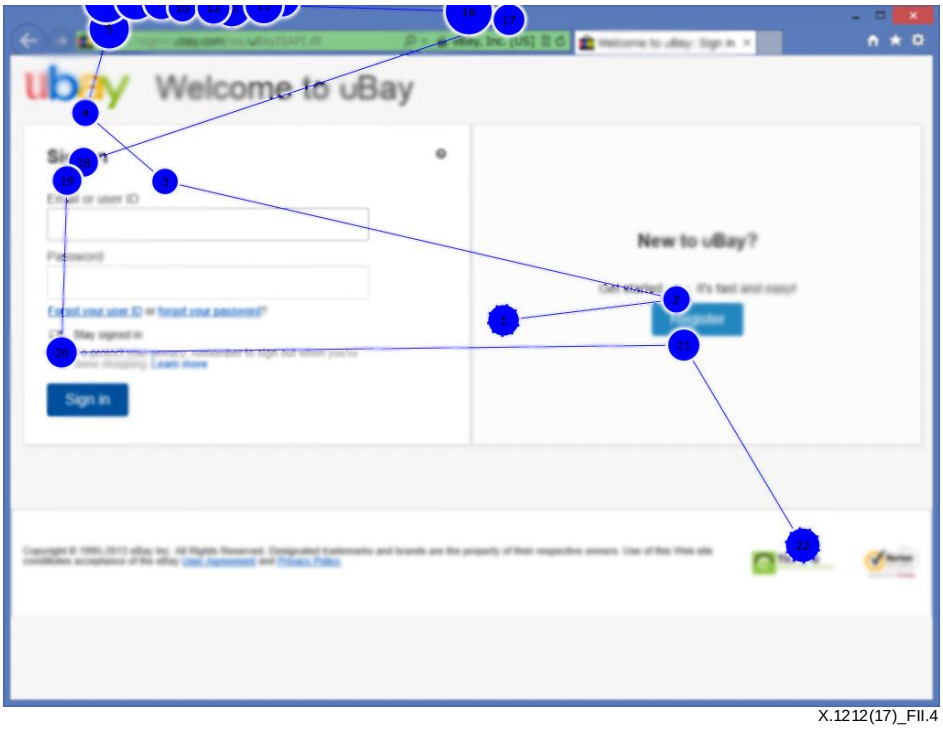



**Figura II.4 – Usuario experto en un sitio web legítimo**

En el caso del sitio web legítimo, el usuario inexperto también prestó atención solamente al contenido web, como se ve en la Figura II.3. Por el contrario, el experto tiende a evaluar el URL del sitio y/o el indicador SSL del navegador, en lugar del contenido de la página web, a la hora de determinar la credibilidad del sitio, como se ve en la Figura II.4. Estas observaciones comportamentales indican que los expertos tienden a mirar la barra de dirección donde aparecen el URL y el indicador SSL al principio de la navegación. Los inexpertos los ignoran por no saber lo que son el URL o los indicadores SSL.

# Bibliografía


[b-UIT-T F.790] Recomendación UIT-T F.790 (2007), *Directrices sobre la posibilidad de acceso a las telecomunicaciones en favor de las personas de edad y las personas con discapacidades.*
<https://www.itu.int/rec/T-REC-F.790>

[b-UIT-T F.791] Recomendación UIT-T F.791 (2015), *Términos y definiciones de accesibilidad*.
<https://www.itu.int/rec/T-REC-F.791>

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones de referencia para la gestión de la identidad*.
<https://www.itu.int/rec/T-REC-X.1252>

[b-UIT-T X.1254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de autentificación de entidad.*
<https://www.itu.int/rec/T-REC-X.1254>

[b-UIT-T X.1500] Recomendación UIT-T X.1500 (2011), *Aspectos generales del intercambio de información de ciberseguridad.*
<https://www.itu.int/rec/T-REC-X.1500>

[b-ITU-T-FSTP-TACL] ITU-T FSTP-TACL (2006), *Telecommunications Accessibility Checklist.*
<https://www.itu.int/publ/T-TUT-FSTP-2006-TACL>

[b-IETF RFC 5901] IETF RFC 5901 (2010), *Extensions to the IODEF-Document Class for Reporting Phishing*.
<http://datatracker.ietf.org/doc/rfc5901/>

[b-IETF RFC 6376] IETF RFC 6376 (2011), *DomainKeys Identified Mail (DKIM) Signatures.*
<http://datatracker.ietf.org/doc/rfc6376/>

[b-ISO/IEC 40500] ISO/IEC 40500:2012, *Information Technology – W3C Web Content Accessibility Guidelines (WCAG) 2.0*.

[b-ANSI-Z535.4] ANSI (2011), Product Safety Signs and Labels.

[b-CAB-Baseline] CA/Browser Forum (2011), *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* Version 1.0.
<http://www.cabforum.org/Baseline_Requirements_V1.pdf>

[b-Crawford] Crawford, T.J., Higham, S., Renvoize, T., Patel, J., Dale, M., Suriya, A., Tetley S. (2005), *Inhibitory control of saccadic eye movements and cognitive impairment in Alzheimer's disease*, Biological Psychiatry, vol. 9, No. 57.

[b-ENISA] ENISA (V6_2, 2011), *Measurement Frameworks and Metrics for Resilient Networks and Services: technical report*.

[b-Felt2014] Felt, A.P., Reeder, R.W., Almuhimedi. H., Consolvo, S. (2014), *Experimenting At Scale With Google Chrome's SSL Warnings*, in Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems.

[b-Felt2015] Felt, A.P., Ainslie, A., Reeder, R.W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., Grimes, J. (2015), *Improving SSL Warnings: Comprehension and Adherence*, in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.

[b-Genno] Genno, H., Ishikawa, K., Kanbara, O., Kikumoto, M., Fujiwara, Y., Suzuki, R., Osumi, M. (1997), *Using facial skin temperature to objectively evaluate sensations*, International Journal of Industrial Ergonomics, vol. 19.

[b-Irwin] Irwin, D.E., Brockmole, J.R. (2000), *Mental rotation is suppressed during saccadic eye movements*, Psychonomic Bulletin and Review, vol. 7, No. 4.

[b-Leigh] Leigh, R.J., Zee, D.S. (1991), *The Neurology of Eye Movements*, 4th ed. Oxford University Press.

[b-Miyamoto] Miyamoto, D., Iimura, T., Tazaki, H., Blanc, G., Kadobayashi, Y. (2014), *EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits*, in Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security.

[b-Noris] Noris, B. Benmachiche, K., Meynet, J., Thiran, J.P., Billard, A. (2007), *Analysis of Head-Mounted Wireless Camera Videos for Early Diagnosis of Autism*, Advances in Soft Computing, vol. 45.

[b-Or] Or, C.K.L., Duffy, V.G. (2007), *Development of a facial skin temperature-based methodology for nonintrusive mental workload measurement*, Occupational Ergonomics, vol. 7.

[b-Rigdon] Rigdon, M., Ishii, K., Watabe, M., and Kitayama, S. (2009), *Minimal social cues in the dictator game*, Journal of Economic Psychology vol. 30, iss. 3.

[b-Senju] Senju, A., Johnson, M.H. (2009), *The eye contact effect: mechanisms and development*, Trend in Cognitive Science.

[b-Tokuda] Tokuda, S., Obinata G., Palmer, E., Chaparro, A. (2011), *Estimation of mental workload using saccadic eye movements in a free-viewing task*, in Proceedings of the 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society.

[b-UNCRPD] Convenciones de las Naciones Unidas sobre los derechos de las personas con discapacidad (2006).

[b-Volskamp] Voskamp, J., Urban, B. (2009), *Measuring Cognitive Workload in Non-military Scenarios Criteria for Sensor Technologies*, in Proceedings of the 5th International Conference on Foundations of Augmented Cognition.

[b-Wang] Wang, L., Duffy V.G., Du, Y. (2007), *A composite measure for the evaluation of mental workload*, in Proceedings of the 1st International Conference on Digital Human Modelling.

## SERIES DE RECOMENDACIONES DEL UIT-T

| | |
|---|---|
| Serie A | Organización del trabajo del UIT-T |
| Serie D | Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales |
| Serie E | Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos |
| Serie F | Servicios de telecomunicación no telefónicos |
| Serie G | Sistemas y medios de transmisión, sistemas y redes digitales |
| Serie H | Sistemas audiovisuales y multimedia |
| Serie I | Red digital de servicios integrados |
| Serie J | Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia |
| Serie K | Protección contra las interferencias |
| Serie L | Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior |
| Serie M | Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes |
| Serie N | Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión |
| Serie O | Especificaciones de los aparatos de medida |
| Serie P | Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales |
| Serie Q | Conmutación y señalización, y mediciones y pruebas asociadas |
| Serie R | Transmisión telegráfica |
| Serie S | Equipos terminales para servicios de telegrafía |
| Serie T | Terminales para servicios de telemática |
| Serie U | Conmutación telegráfica |
| Serie V | Comunicación de datos por la red telefónica |
| **Serie X** | **Redes de datos, comunicaciones de sistemas abiertos y seguridad** |
| Serie Y | Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes |
| Serie Z | Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación |

Impreso en Suiza
Ginebra, 2017