

Objetivo del estudio

El objetivo de este estudio es analizar la percepción y nivel de conocimiento de los usuarios encuestados respecto a seis elementos críticos de control relacionados con la seguridad en el uso de Internet, los elementos de control seleccionados fueron: phishing, uso de contraseñas fuertes, actualización y mantenimiento del sistema operativo, uso de redes wifi seguras, prácticas de seguridad en redes sociales, y uso responsable de aplicaciones y permisos.

Asimismo, se busca relacionar cada elemento crítico (ECSI) con los principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Con base en los resultados obtenidos, se pretende identificar las posibles causas de los comportamientos detectados, con el fin de proponer un plan de acción orientado a mejorar la madurez en seguridad digital de los usuarios.

Representación y descripción del "Universo" evaluado.

Objeto evaluado: Prácticas de seguridad digital en el uso cotidiano de dispositivos por parte de los usuarios encuestados.

Descripción: Se incluyen dispositivos como celulares, laptops y equipos de escritorio utilizados por los usuarios encuestados, tanto para fines personales como laborales, en el contexto de actividades cotidianas relacionadas con el uso de internet y redes sociales.

Importancia: Comprender el nivel de seguridad en el uso cotidiano de estos dispositivos permite identificar vulnerabilidades potenciales y proponer medidas preventivas que minimicen los riesgos de ataques informáticos o pérdida de información.

Alcance de la auditoría: Evaluación de la percepción de los usuarios sobre sus prácticas de seguridad digital, especialmente en cuanto a configuración de dispositivos, uso de contraseñas, acceso a redes seguras y hábitos en redes sociales.

Descripción de los usuarios evaluados.

El 90% de los evaluados son miembros de una organización financiera, las muestras tomadas entre los mismos son elementos que se encuentran en áreas administrativas tales como (analítica, normatividad, auditoría y direcciones) y del área de tecnologías se tomaron en cuenta a 2 miembros del área de ciberseguridad y al equipo completo de soporte técnico, el 10% restante fueron muestras tomadas de nuestras familias, las cuales conocemos no tienen un mínimo de conocimiento tecnológico lo cual nos dio la esperanza de tener muestras variadas. Todos los evaluados entran en un rango de 22 a 57 años de edad.

Identificación y etiqueta de los Elementos Críticos de Control presentes, bajo el siguiente criterio; "ECSI-##"

ECSI-01. Phishing

ECSI-02. Uso de contraseñas fuertes

ECSI-03. Actualización y mantenimiento de sistema operativo

ECSI-04. Wifi-Fi seguras

ECSI-05. Prácticas de seguridad en redes sociales

ECSI-06. Uso responsable de aplicaciones y permisos

Identificación del elemento de la seguridad de la información que está ligado el ECSI que se definió.

Código	Elemento Crítico de Control	Principio(s) Afectado(s)	Justificación
ECSI-01	Phishing	Confidencialidad	El objetivo principal del phishing es obtener acceso no autorizado a información sensible.
ECSI-02	Uso de contraseñas fuertes	Confidencialidad	Contraseñas débiles facilitan accesos indebidos a datos protegidos.
ECSI-03	Actualización y mantenimiento del sistema operativo	Confidencialidad, Integridad y Disponibilidad	Las actualizaciones previenen vulnerabilidades que pueden comprometer todos los pilares CIA.
ECSI-04	Redes wifi seguras	Confidencialidad, Disponibilidad	Una red Wi-Fi insegura puede permitir espionaje (confidencialidad) o denegación de servicio (disponibilidad).
ECSI-05	Prácticas de seguridad en redes sociales	Confidencialidad e Integridad	La sobreexposición puede revelar datos sensibles (confidencialidad) o permitir manipulación de contenido (integridad).
ECSI-06	Uso responsable de aplicaciones y permisos	Confidencialidad e Integridad	El exceso de permisos puede permitir acceso indebido a datos (confidencialidad) o su alteración (integridad).

Descripción de cada Elemento Crítico de Control el análisis obtenido.

Código	Elemento Crítico de Control	Promedio de cumplimiento	Análisis obtenido
ECSI-01	Phishing	83.9%	La mayoría de los usuarios reconoce y aplica buenas prácticas para evitar fraudes de tipo phishing (verifican enlaces, detectan correos falsos y evalúan seguridad de sitios).
ECSI-02	Uso de contraseñas fuertes	86.2%	Alto nivel de conciencia sobre contraseñas seguras, aunque hay oportunidades de mejora en el uso de claves distintas por cuenta.
ECSI-03	Actualización y mantenimiento de sistema operativo	41.4%	Se identifica una debilidad considerable: varios usuarios ignoran actualizaciones o no reconocen los riesgos asociados a no realizarlas.
ECSI-04	Redes wifi seguras	65.5%	Prácticas mixtas: aunque muchos cambian contraseñas por defecto, aún hay exposición al uso de redes públicas o compartir contraseñas libremente.
ECSI-05	Seguridad en redes sociales	28.7%	Bajo nivel de prácticas seguras: varios perfiles son públicos o se comparte información personal. Requiere atención prioritaria.
ECSI-06	Uso responsable de aplicaciones y permisos	57.5%	Más de la mitad revisa permisos y elige fuentes oficiales, pero aún existe riesgo por instalación ocasional de apps fuera de tiendas confiables.

Descripción de la posible "Causa" del escenario analizado.

Código	Elemento Crítico de Control (ECSI)	Descripción del Elemento	Posible Causa Identificada
ECSI-01	Phishing	Riesgo de suplantación de identidad mediante correos o enlaces falsos.	Aunque el nivel de conocimiento es alto, persiste un pequeño grupo que aún no distingue señales avanzadas de suplantación, posiblemente por falta de entrenamiento práctico o actualización en nuevas tácticas de fraude.
ECSI-02	Uso de contraseñas fuertes	Protección de cuentas mediante contraseñas robustas y únicas.	El buen resultado muestra concientización general, pero puede haber usuarios que repiten contraseñas o no utilizan gestores, lo cual podría

			deberse a hábitos adquiridos o falta de confianza en herramientas.
ECSI-03	Actualización del sistema operativo	Mantenimiento y parches de seguridad en sistemas usados.	La baja adopción de actualizaciones refleja una posible falta de comprensión sobre su impacto en la seguridad o desinterés ante interrupciones del sistema durante el proceso de actualización.
ECSI-04	Redes wifi seguras	Configuración adecuada de redes inalámbricas, personales o corporativas.	El cumplimiento intermedio indica que algunos usuarios aún utilizan redes públicas o contraseñas débiles, posiblemente por comodidad, desconocimiento técnico o subestimación del riesgo.
ECSI-05	Seguridad en redes sociales	Gestión de privacidad, contenido compartido y exposición de información.	La causa principal parece ser desconocimiento sobre configuración de privacidad y exposición involuntaria de información personal, influida por la percepción errónea de que "no hay nada que ocultar".
ECSI-06	Uso responsable de aplicaciones y permisos	Evaluación de accesos concedidos a apps (ubicación, cámara, contactos, etc.).	Aunque hay prácticas aceptables, se observa una tendencia a aceptar permisos sin leer, debido a la confianza ciega en las apps o prisa al instalar, así como desconocimiento de los riesgos asociados.

Descripción de un posible "Plan de acción" ante el escenario analizado.

Código	Elemento crítico de control	Acción correctiva	Responsable sugerido	Prioridad	Indicador
ESCI-01	Phishing	Realizar talleres semestrales sobre detección de correos y enlaces fraudulentos.	Área de ciberseguridad	Media	Aumento del reconocimiento de intentos de phishing en simulaciones internas.
ESCI-02	Contraseñas fuertes	Fomentar el uso de gestores de contraseñas mediante campañas internas y guías visuales	Soporte técnico	Media	Disminución en la repetición de contraseñas en cuentas distintas.
ECSI-03	Actualización del sistema operativo	Implementar alertas automáticas que	Departamento de TI	Alta	Incremento de porcentaje de usuarios con sistema

		expliquen los riesgos de no actualizar y facilitar actualizaciones con horarios definidos.			actualizado.
ECSI-04	Redes wi-fi seguras	Crear cápsulas informativas sobre riesgos de redes públicas y cómo configurar el Wi-Fi de forma segura.	Área de ciberseguridad	Media	Reducción en el uso de redes no protegidas.
ECSI-05	Seguridad en redes sociales	Elaborar guías digitales sobre la privacidad en redes sociales y realizar auditorías aleatorias de configuración.	Recursos humanos y ciberseguridad	Alta	Aumento en el número de perfiles con privacidad reforzada.
ECSI-06	Permisos y uso responsable de apps	Realizar campañas de concientización sobre permisos sensibles, con ejemplos de apps maliciosas y buenas prácticas	Soporte Técnico	Alta	Reducción del número de instalaciones fuera de tiendas oficiales.

Descripción del nivel de madurez que se detecta en los usuarios con respecto a su seguridad en el uso de internet.

El nivel de madurez de los usuarios en cuanto a seguridad en el uso de Internet es intermedio, con puntos fuertes y áreas críticas que requieren atención, ya que la mayoría de los usuarios evaluados muestran una buena conciencia básica de los elementos críticos de control que se eligieron, sin embargo, también se detectan debilidades importantes en las áreas de mantener los dispositivos actualizados, proteger adecuadamente sus redes wifi, y especialmente en el uso de redes sociales y permisos de aplicaciones, donde muchos usuarios no son conscientes del riesgo o no saben cómo configurarlos correctamente.