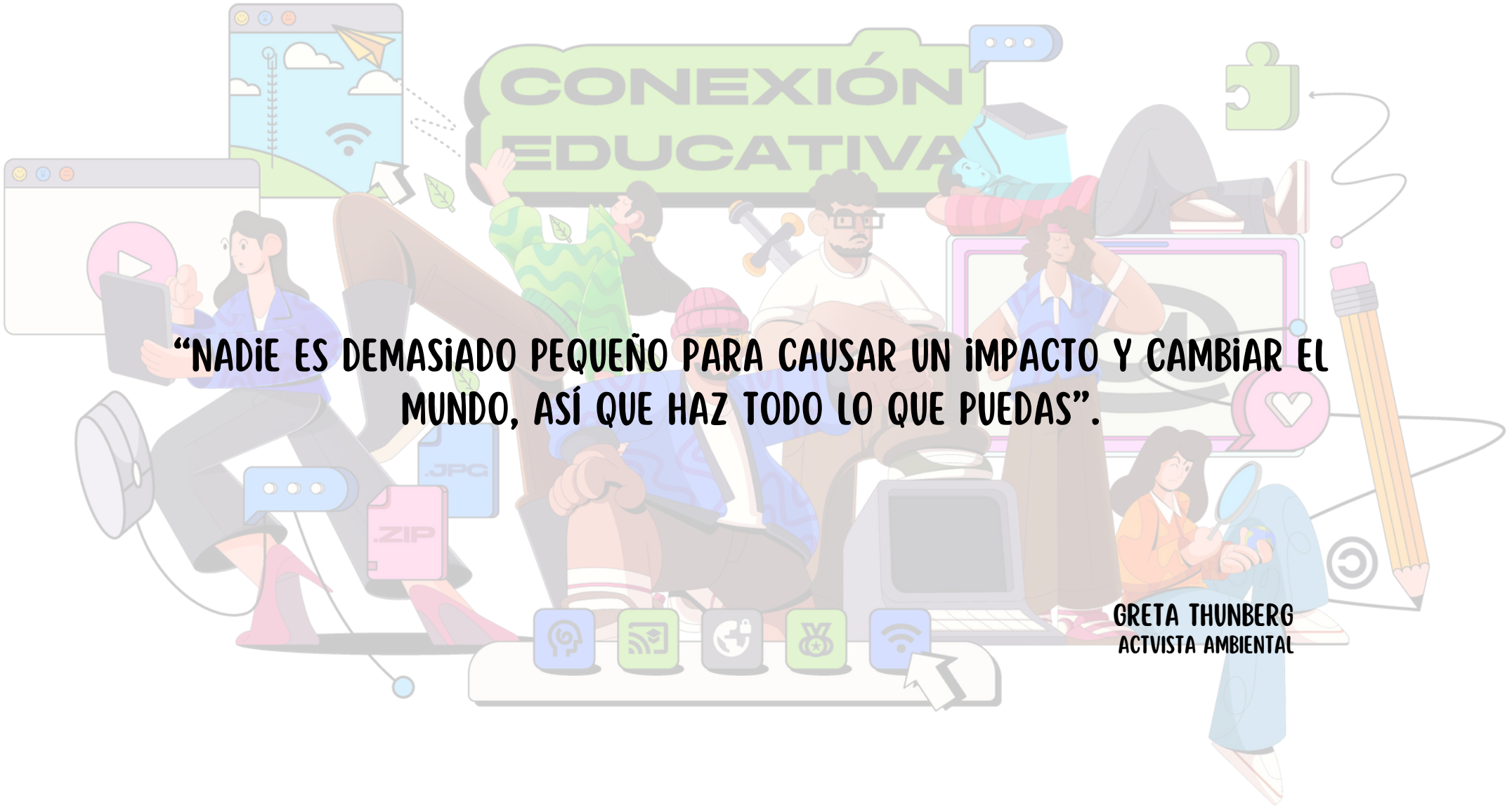
@conexioneduec

ACOMPAÑAMIENTO HOLÍSTICO PARA LA PREVENCIÓN DE RIESGOS DIGITALES Y PSICOSOCIALES EN ORGANIZACIONES DE LA SOCIEDAD CIVIL.



"NADIE ES DEMASIADO PEQUEÑO PARA CAUSAR UN IMPACTO Y CAMBIAR EL MUNDO, ASÍ QUE HAZ TODO LO QUE PUEDAS".

GRETA THUNBERG
ACTVISTA AMBIENTAL

LÍNEAS DE ACCIÓN

- **Tecnologias libres y educacion**

Generamos espacios de formación para el uso crítico de tecnologías responsables basados en los principios de la Educación Popular.

- **Seguridad Digital**

Brindamos acompañamiento a la sociedad civil para mejorar sus prácticas de seguridad digital, apaliar la violencia de género en línea y promover derechos digitales.

- **Autocuidado**

Fomentamos la importancia de ser consciente de los pensamientos y emociones brindando ayuda oportuna en casos de riesgos digitales, mediante la psicoeducación y acompañamiento, que permita el desarrollo integral con un enfoque en la tecnología feminista.

- **Liderazgo y Proyectos**

Incentivamos en las y los jóvenes la generación de ideas innovadoras, fomentando el trabajo en equipo y la motivación para tener un desenvolvimiento pleno en su diario vivir.

- **EcoInnovación**

Desarrollar soluciones creativas orientadas hacia la sostenibilidad ambiental. Reducir la huella ecológica y promover la conservación de recursos naturales en todas nuestras actividades.

EJES TRANSVERSALES

- **Diversidad y equidad de género**

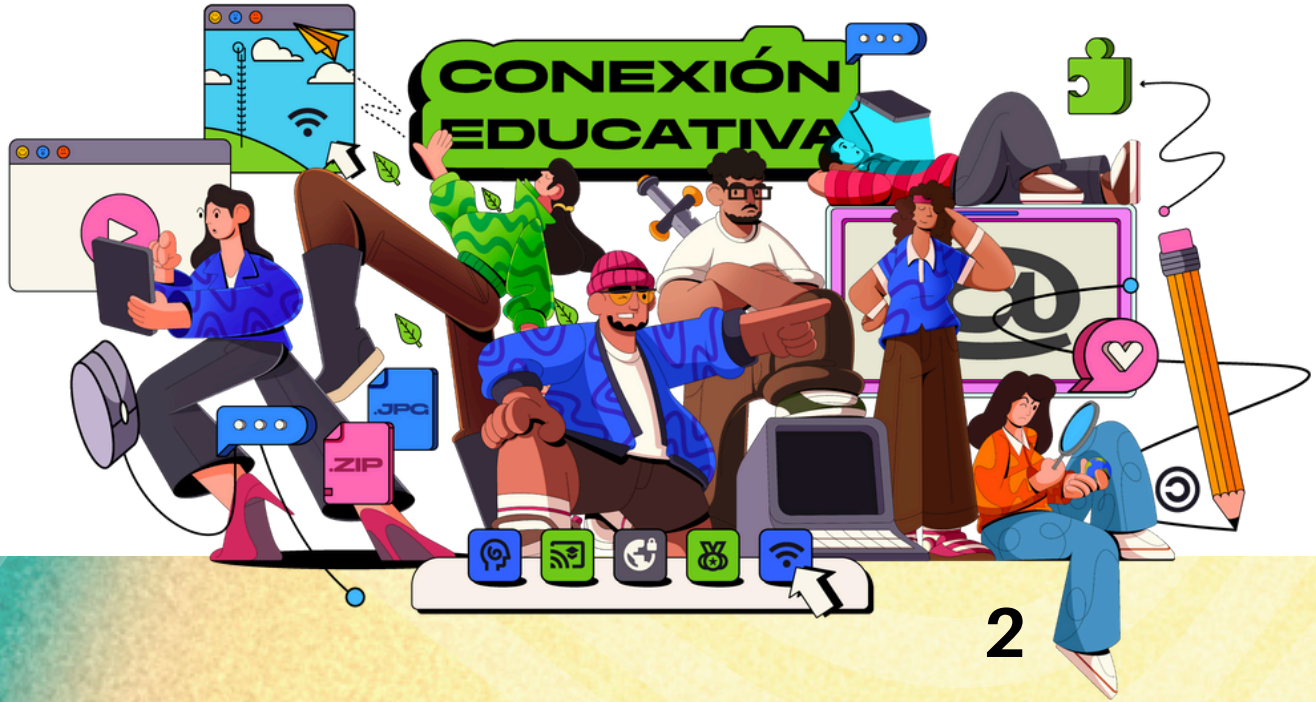
Nuestros espacios de formación y de acompañamiento se articulan aceptando la diversidad y equidad de género de nuestras beneficiarias.

- **Derechos Humanos, justicia social y antirracismo**

Los derechos humanos son la base fundamental de nuestros procesos, por lo tanto, enfocamos nuestro trabajo en organizaciones de base de pueblos y nacionalidades indígenas y afrodescendientes, activistas, grupos feministas, defensoras de derechos humanos, personas LGBTIQ+, Comunicadoras, entre otras.

¿QUIÉNES SOMOS?

Somos una organización sin fines de lucro que promueve los derechos humanos y la justicia social por medio del intercambio de conocimiento, investigación y acompañamiento en la implementación de tecnologías digitales con un enfoque crítico y participativo, para lograrlo conectamos diferentes líneas de acción y ejes transversales.



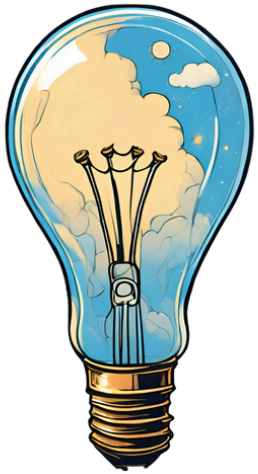
OBJETIVOS DEL MANUAL

Objetivo General

Proporcionar herramientas que faciliten la realización del diagnostico técnico y psicosocial a las organizaciones de la sociedad civil.

¿A quién va dirigido?

- Instructores de seguridad Digital
- Organizaciones sociales que realizan acompañamiento en seguridad digital
- Auditores de seguridad digital
- Personas interesadas en comprender procesos de acompañmamiento en seguridad digital



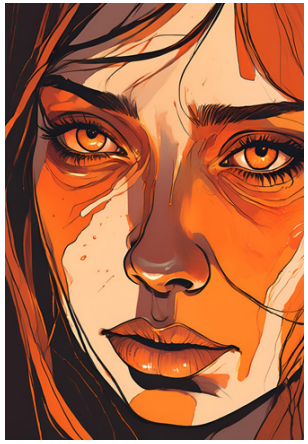
CONCEPTOS CLAVE

- **¿Qué son los riesgos Psicosociales?**

Las activistas, voluntarias y defensoras de derechos humanos, al dedicarse a causas sociales, pueden enfrentarse a una serie de riesgos psicosociales que impactan su bienestar mental y emocional. Estos riesgos dependen del tipo de causa que apoyan, del entorno en el que se desenvuelven y del grado de compromiso que asumen. Entre los riesgos psicosociales más comunes se encuentran:

- **Sobrecarga emocional:** Acumulación de tensiones derivadas de la intensidad emocional que conlleva el trabajo en causas sensibles.

- **Culpa y frustración:** Sentimientos de impotencia cuando los resultados no son los esperados o no se puede ayudar como se quisiera.



- **Estigmatización y hostigamiento:** Ser blanco de críticas, ataques o aislamiento por su activismo.

- **Burnout:** Agotamiento físico, mental y emocional debido a la exposición prolongada al estrés.

- **Trauma secundario:** Efectos traumáticos derivados de escuchar, presenciar o estar inmerso en situaciones extremas de vulneración de derechos.

La exposición continua a situaciones emocionalmente desgastantes, estresantes o traumáticas puede comprometer seriamente la salud mental y el bienestar emocional de quienes trabajan en la defensa de derechos, lo que resalta la importancia de implementar estrategias de autocuidado y apoyo psicosocial.

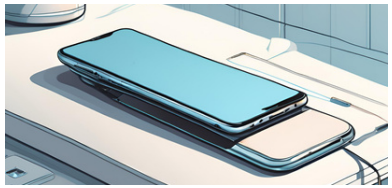
CONCEPTOS CLAVE

¿Qué son los Riesgos Digitales?

Los riesgos digitales son amenazas que surgen del uso de tecnologías digitales y representan un peligro creciente para la seguridad de la información en línea. Estos riesgos pueden provenir de diversas fuentes, tanto externas como internas, y se manifiestan en ataques cibernéticos como:

- **Hackeos dirigidos:** Ataques personalizados con el fin de obtener acceso no autorizado a sistemas o información confidencial.
- **Virus y malware:** Programas maliciosos diseñados para dañar o comprometer dispositivos y redes.

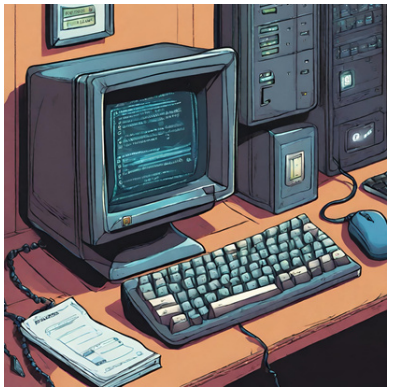
- **Phishing:** Estrategias fraudulentas para engañar a los usuarios y robar credenciales o información personal.
- **Robo de identidad:** Usurpación de la identidad de una persona para acceder a sus recursos o cometer fraudes.
- **Espionaje en línea:** Vigilancia no autorizada de actividades en la red para obtener datos sensibles.



- **Exposición de datos personales:** La divulgación involuntaria o maliciosa de información privada debido al mal uso de herramientas tecnológicas.

En la era digital actual, donde tanto individuos como organizaciones dependen de la tecnología para realizar tareas cotidianas como banca en línea, compras virtuales y almacenamiento de datos, los riesgos digitales son cada vez más comunes.

Para reducir estos peligros, es fundamental adoptar medidas de seguridad informática robustas y mantenerse constantemente alerta ante nuevas amenazas.



METODOLOGÍA ACTIVA:

La metodología ACTIVA es un enfoque desarrollado para apoyar a las Organizaciones de la Sociedad Civil (OSC) en la prevención de riesgos digitales y psicosociales. Este método sigue un ciclo de intervención estructurado que busca fomentar el aprendizaje, la implementación y la mejora continua para fortalecer tanto la seguridad como el bienestar organizacional.

DESCRIPCIÓN DE LAS FASES DE ACTIVA:

1. Análisis y diagnóstico

Esta fase es crucial para conocer las particularidades de la organización, sus necesidades y los riesgos a los que está expuesta. Se basa en el principio de que el diálogo abierto y el análisis detallado son fundamentales para diseñar intervenciones efectivas.

METODOLOGÍA ACTIVA

- **Objetivo:** Evaluar el estado actual de la organización en cuanto a riesgos digitales y psicosociales.
- **Actividades:** Recolección de información a través de entrevistas, encuestas y reuniones con los líderes y colaboradores clave. Identificación de amenazas y vulnerabilidades mediante metodología SAFETAG y aplicación de técnicas OSINT.
- **Resultados esperados:** Un diagnóstico claro de la situación de la organización y la definición de los riesgos prioritarios a abordar.

2. Creación de espacios formativos
Con base en el diagnóstico realizado, se diseñan espacios de formación adaptados a las necesidades detectadas. Estos espacios deben facilitar el aprendizaje continuo y generar conciencia sobre la importancia de la seguridad digital y el bienestar psicosocial.

- **Objetivo:** Capacitar a los miembros de la organización en temas clave para la prevención de riesgos.
- **Actividades:** Talleres, cursos, seminarios y capacitaciones sobre ciberseguridad, manejo del estrés, resolución de conflictos y otros temas relevantes.
- **Resultados esperados:** Un equipo capacitado y consciente de los riesgos y de las buenas prácticas a seguir para minimizarlos.

3. Tareas prácticas
La fase de tareas prácticas busca trasladar lo aprendido en los espacios formativos a la vida cotidiana de la organización. La idea es que los participantes puedan aplicar los conocimientos adquiridos para enfrentar situaciones reales y mejorar los procesos internos.

- **Objetivo:** Implementar lo aprendido a través de ejercicios prácticos que simulan escenarios reales.
- **Actividades:** Simulacros de ataques cibernéticos, creación de protocolos de seguridad, identificación de señales de riesgo psicosocial, etc.
- **Resultados esperados:** Integración de buenas prácticas en la rutina diaria de la organización, desarrollando una cultura preventiva.

4. Implementación

Esta fase consiste en la formalización de las medidas diseñadas durante el proceso de capacitación y práctica. Aquí, se establecen protocolos permanentes que permitan a la organización estar mejor preparada frente a los riesgos digitales y psicosociales.

- **Objetivo:** Integrar formalmente las acciones de prevención en los procesos operativos de la organización.
- **Actividades:** Definición de políticas internas, asignación de roles y responsabilidades, implementación de herramientas tecnológicas para la prevención.
- **Resultados esperados:** Procedimientos y políticas claras que guíen las acciones preventivas y reactivas ante posibles amenazas.

5. Valoración

La evaluación del proceso y de los resultados es fundamental para determinar la eficacia de las acciones implementadas. En esta fase, se revisa si los objetivos se han alcanzado y qué aspectos requieren ajustes.

- **Objetivo:** Medir el impacto de las medidas adoptadas y su efectividad.
- **Actividades:** Auditorías, encuestas de satisfacción, revisión de indicadores clave de desempeño (KPIs).
- **Resultados esperados:** Un reporte que evalúe los logros alcanzados y las áreas que necesitan mejora.

6. Ajuste y mejora

Finalmente, el ciclo ACTIVA promueve la mejora continua a través de la retroalimentación. Con base en los resultados de la valoración, se ajustan las estrategias y se refuerzan las acciones que han demostrado ser efectivas.

- **Objetivo:** Mejorar continuamente las políticas y prácticas adoptadas, adaptándose a los nuevos retos y riesgos que puedan surgir.

- **Actividades:** Revisiones periódicas, actualización de protocolos, nuevos ciclos formativos según las necesidades emergentes.

- **Resultados esperados:** Una organización más resiliente, con una cultura de prevención sólida y capacidad de adaptación.

7: Cierre

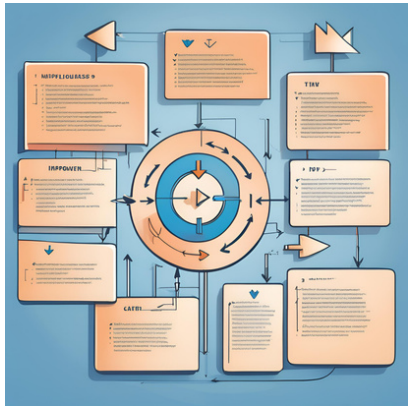
En esta fase procedemos a dar por finalizado el proyecto y las organizaciones sociales evalúan el acompañamiento que se tuvo durante la ejecución del proyecto. También se realiza una evaluación interna sobre el cumplimiento de las actividades que realizó la organización auditora.

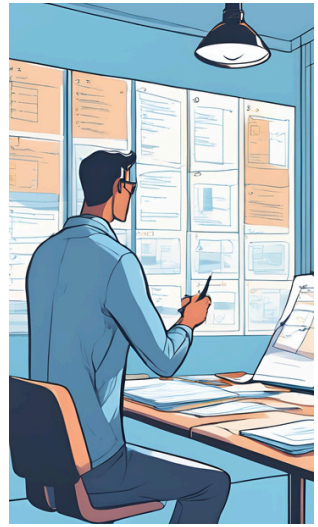
- **Matriz Evaluación del proyecto**

Herramienta que puede ser empleada en actividades presenciales o virtuales. La herramienta recopila información cualitativa y cuantitativa del accionar de los facilitadores del proyecto. Anexo

- **Matriz de Evaluación interna**

Permite evidenciar si se cumplió con la actividad, identificando si se tuvo un uso eficiente de recursos, uso correcto de tiempos, permite identificar el cumplimiento de actividades. Anexo



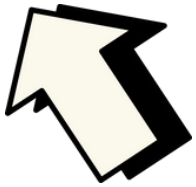


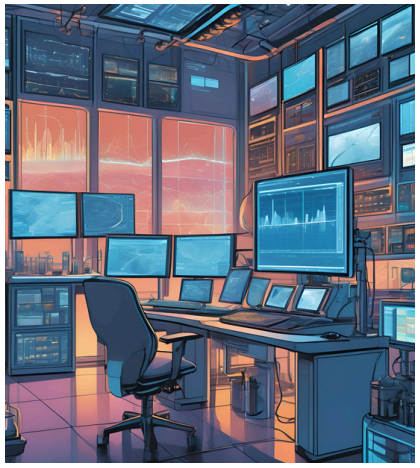
ANÁLISIS Y DIAGNÓSTICO INICIAL

El Análisis y Diagnóstico Inicial es la primera fase dentro del proceso de acompañamiento en la prevención de riesgos digitales y psicosociales en las Organizaciones de la Sociedad Civil (OSC). En esta fase, se busca comprender en profundidad las características particulares de la organización, sus dinámicas internas, y el contexto en el que opera. Este análisis es fundamental para identificar los riesgos y vulnerabilidades a los que se enfrenta la organización, tanto a nivel digital como psicosocial.

En la fase de Análisis y Diagnóstico Inicial, se busca obtener un conocimiento profundo de las particularidades y necesidades de la organización, además de identificar los riesgos a los que está expuesta, tanto a nivel digital como psicosocial.

Esta etapa es crítica porque a partir de un diálogo abierto y un análisis detallado se puede diseñar un plan de intervención adecuado y efectivo.





El proceso comienza con la recolección de información mediante entrevistas, encuestas y reuniones con los líderes y colaboradores clave de la organización.

Este intercambio de información debe realizarse en un ambiente de confianza, donde las personas puedan expresar libremente sus preocupaciones y percepciones. La identificación de riesgos se lleva a cabo utilizando herramientas como SAFETAG, que permite auditar y evaluar la seguridad digital de manera integral. Asimismo, se utilizan técnicas OSINT para identificar amenazas externas a través de la exploración de fuentes de información abiertas.

El objetivo final es obtener un diagnóstico claro que identifique vulnerabilidades y amenazas, junto con una comprensión del contexto organizacional. Esto permitirá diseñar acciones preventivas y correctivas adaptadas, siendo clave el detalle y precisión del análisis para futuras intervenciones.

CREACIÓN DE ESPACIOS FORMATIVOS

La **Creación de espacios formativos** es una etapa fundamental para garantizar que los miembros de la organización no solo comprendan los riesgos a los que están expuestos, sino que también adquieran las herramientas necesarias para enfrentarlos de manera efectiva.

A partir del diagnóstico obtenido en la fase anterior, se desarrollan programas de formación que responden a las necesidades específicas de la organización, con el fin de promover el **aprendizaje continuo** y fortalecer la conciencia sobre la seguridad digital y el bienestar psicosocial.

El enfoque formativo está diseñado para abordar temas clave relacionados con la prevención de riesgos, tales como **ciberseguridad, manejo del estrés, y resolución de conflictos**.

Los métodos de capacitación pueden incluir talleres interactivos, seminarios y cursos especializados que promuevan la participación activa de los integrantes.

Estos espacios no solo buscan transferir conocimientos, sino también generar una **reflexión crítica** sobre la importancia de adoptar buenas prácticas que protejan tanto el entorno digital como el entorno emocional de la organización.

El resultado esperado es contar con un equipo capacitado, capaz de identificar riesgos y aplicar las buenas prácticas aprendidas para reducir vulnerabilidades. De esta forma, se fomenta una cultura preventiva que refuerza tanto la seguridad técnica como el bienestar psicosocial dentro de la organización.

TAREAS PRÁCTICAS

Las tareas prácticas son fundamentales para asegurar que el aprendizaje teórico se traduzca en acciones concretas que mejoren la seguridad y el bienestar en la organización. Esta fase permite a los participantes aplicar los conocimientos adquiridos en situaciones reales, ayudando a fortalecer la resiliencia y la capacidad de respuesta ante los riesgos digitales y psicosociales.

1. Creación de Políticas de Seguridad Digital

Una de las tareas prácticas clave es el desarrollo e implementación de políticas de seguridad digital. Estas políticas proporcionan un marco claro para proteger la información y los recursos tecnológicos de la organización. Aquí se detallan los pasos para su creación:

- **Evaluación de Necesidades:** Identifica los riesgos digitales específicos a los que está expuesta la organización y las necesidades de seguridad. Esto puede incluir la protección de datos sensibles, la gestión de accesos y la prevención de ataques cibernéticos.

- **Redacción de Políticas:** Desarrolla políticas claras y detalladas que cubran aspectos críticos como:

  - **Control de Acceso:** Define cómo se gestionan los permisos y accesos a sistemas y datos.

  - **Protección de Datos:** Establece medidas para el cifrado y almacenamiento seguro de datos.
  - **Uso Aceptable:** Define las normas para el uso de dispositivos y redes.
  - **Respuesta a Incidentes:** Detalla los procedimientos para responder a posibles brechas de seguridad.

- **Implementación y Comunicación:** Asegúrate de que las políticas sean comunicadas de manera efectiva a todos los miembros de la organización. Proporciona capacitación para garantizar que comprendan y sigan las nuevas directrices.

2. Gestión de Riesgos Psicosociales

La implementación de medidas para abordar los riesgos psicosociales es igualmente crucial. Las tareas prácticas en esta área se centran en crear un entorno de trabajo saludable y resiliente. Los pasos incluyen:

- Evaluación del Entorno Psicosocial: Realiza una evaluación para identificar las fuentes de estrés, las señales de agotamiento y otros riesgos psicosociales en la organización. Utiliza encuestas, entrevistas y grupos focales para obtener información.

- Desarrollo de Estrategias de Apoyo: Diseña estrategias para abordar los problemas identificados, como:
    - Programas de Bienestar: Implementa iniciativas para promover la salud mental, como talleres de manejo del estrés y programas de apoyo psicológico.
    - Protocolos de Comunicación: Establece canales de comunicación abiertos para que los empleados puedan expresar preocupaciones y recibir apoyo.

    - Políticas de Equilibrio Trabajo-Vida: Desarrolla políticas que promuevan un equilibrio saludable entre la vida laboral y personal, como horarios flexibles y días de descanso.

- Capacitación y Sensibilización: Organiza sesiones de capacitación sobre salud mental y manejo del estrés para aumentar la conciencia y la comprensión entre los miembros de la organización.

- Evaluación y Ajuste: Monitorea el impacto de las medidas implementadas y realiza ajustes según sea necesario para abordar nuevas necesidades o problemas emergentes.

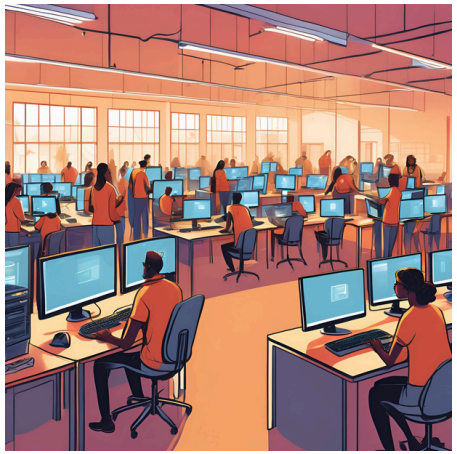
IMPLEMENTACIÓN

La fase de **Implementación** es crucial para llevar a la práctica las políticas y estrategias diseñadas durante la fase de tareas prácticas. En el contexto de organizaciones de la sociedad civil, donde la mayoría de los participantes son voluntarios o miembros, esta fase se enfoca en asegurar que todos los involucrados comprendan y apliquen las nuevas políticas y cambios necesarios para enfrentar los riesgos identificados.

1. Aplicación de Políticas de Seguridad Digital

- **Difusión de Políticas:** Comparte las políticas de seguridad digital con todos los voluntarios y miembros de la organización. Utiliza plataformas accesibles, como correos electrónicos, reuniones virtuales, boletines informativos y grupos de comunicación en redes sociales.
- **Capacitación Adaptada:** Organiza sesiones de capacitación específicas para voluntarios y miembros. Estas sesiones deben ser interactivas y prácticas, enfocándose en cómo aplicar las políticas de seguridad digital en sus roles y actividades.

Organiza sesiones de capacitación específicas para voluntarios y miembros.



Estas sesiones deben ser interactivas y prácticas, enfocándose en cómo aplicar las políticas de seguridad digital en sus roles y actividades. Considera usar talleres breves o módulos en línea que se adapten a sus horarios flexibles.

- **Implementación de Herramientas de Seguridad:** Facilita el acceso a herramientas y recursos necesarios para mantener la seguridad digital, como software de protección y guías para su uso. Proporciona apoyo técnico para la instalación y configuración si es necesario.
- **Monitoreo y Soporte:** Establece mecanismos de apoyo para responder a consultas y problemas relacionados con la seguridad digital.

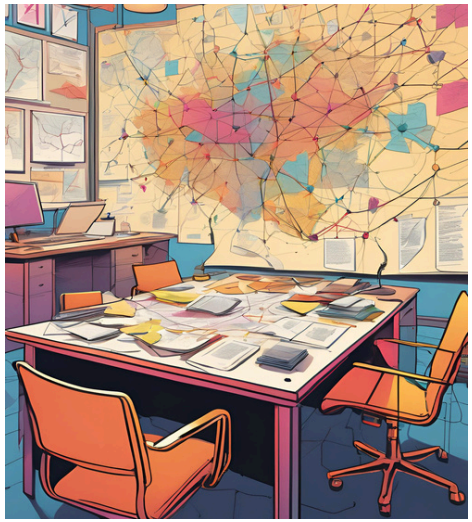
Utiliza grupos de discusión o redes de soporte dentro de la organización para facilitar la resolución de problemas y el cumplimiento de las políticas.

2. Implementación de Cambios Psicosociales

- Aplicación de Estrategias de Apoyo: Introduce las estrategias diseñadas para mejorar el bienestar psicosocial entre los voluntarios y miembros. Esto puede incluir actividades de grupo para fomentar el apoyo mutuo, talleres sobre manejo del estrés y recursos para la salud mental.

- Capacitación y Sensibilización: Organiza actividades formativas que aumenten la conciencia sobre la importancia del bienestar psicosocial y brinden herramientas prácticas para gestionarlo. Utiliza métodos flexibles que se adapten a los horarios y disponibilidades de los voluntarios.

- Revisión Continua: Evalúa periódicamente la efectividad de las políticas implementadas mediante encuestas a los voluntarios y revisiones de las prácticas de seguridad.



Ajusta las políticas y procedimientos basándote en la retroalimentación y las nuevas amenazas identificadas.

- **Promoción de un Entorno Positivo:** Fomenta un ambiente de trabajo colaborativo y de apoyo, donde los voluntarios y miembros se sientan valorados y comprendidos. Implementa prácticas que promuevan el equilibrio entre las actividades de la organización y la vida personal.

- **Facilitación de la Comunicación:** Establece canales de comunicación accesibles donde los voluntarios y miembros puedan expresar sus preocupaciones y recibir apoyo. Considera usar plataformas digitales que sean cómodas y familiares para todos.

- **Evaluación de Impacto:** Recoge feedback sobre las iniciativas psicosociales mediante encuestas y conversaciones informales. Analiza esta información para medir el impacto de las medidas implementadas y ajusta las estrategias según sea necesario.

- **Ajuste y Mejoras:** Realiza ajustes en las estrategias psicosociales basados en la evaluación continua. Mantén un enfoque flexible para adaptar las medidas a las necesidades cambiantes de los voluntarios y miembros.

3. Integración de Políticas y Estrategias

- Coordinación entre Seguridad Digital y Bienestar Psicosocial: Asegúrate de que las políticas de seguridad digital y las estrategias de bienestar psicosocial se complementen y respalden mutuamente. Una integración efectiva contribuirá a un entorno seguro y saludable para todos los involucrados.

- Desarrollo de Protocolos de Respuesta: Crea protocolos para gestionar incidentes que puedan afectar tanto la seguridad digital como el bienestar psicosocial de los voluntarios y miembros. Asegúrate de que estos protocolos sean claros y accesibles.

- Comunicación Continua: Mantén a los voluntarios y miembros informados sobre las políticas y estrategias mediante comunicaciones regulares. Refuerza la importancia de seguir las directrices y participar en las actividades de apoyo disponibles.

VALORACIÓN

La fase de Valoración es fundamental para evaluar la efectividad de las políticas y estrategias implementadas. En esta etapa, se revisa el impacto de las medidas adoptadas para asegurar que se estén cumpliendo los objetivos de seguridad digital y bienestar psicosocial. La valoración permite identificar áreas de mejora y ajustar las estrategias para maximizar su eficacia.

A continuación, se detallan los pasos clave para una valoración efectiva en el contexto de organizaciones de la sociedad civil:

1. Recolección de Datos

- Encuestas y Cuestionarios: Diseña y distribuye encuestas a los voluntarios y miembros para obtener su opinión sobre la efectividad de las políticas y estrategias implementadas. Incluye preguntas sobre la facilidad de aplicación, la utilidad de las herramientas proporcionadas y el impacto en su bienestar.
- Entrevistas y Grupos Focales: Realiza entrevistas y sesiones de grupos focales para obtener una comprensión más profunda de las experiencias y percepciones de los participantes. Estas discusiones pueden revelar aspectos cualitativos que las encuestas no capturan completamente.

2. Análisis de Resultados

- Evaluación del Cumplimiento: Revisa el grado de cumplimiento de las políticas de seguridad digital y las estrategias psicosociales. Determina si los voluntarios y miembros están siguiendo las prácticas establecidas y si las herramientas y recursos están siendo utilizados adecuadamente.

VALORACIÓN

- Impacto en el Bienestar: Evalúa el impacto de las iniciativas psicosociales en el bienestar general de los participantes. Considera aspectos como la reducción del estrés, la mejora de la comunicación y el aumento de la satisfacción y el compromiso.

3. Retroalimentación y Ajustes

- Revisión de Retroalimentación: Recoge y analiza la retroalimentación proporcionada por los voluntarios y miembros. Identifica áreas de mejora y ajusta las políticas y estrategias en función de los comentarios recibidos.
- Ajuste de Políticas: Modifica las políticas de seguridad digital y las estrategias psicosociales para abordar cualquier deficiencia identificada. Asegúrate de que los cambios sean comunicados claramente a todos los involucrados.
- Actualización de Herramientas y Recursos: Realiza actualizaciones en las herramientas y recursos utilizados para apoyar la seguridad digital y el bienestar psicosocial. Esto puede incluir la implementación de nuevas tecnologías, la mejora de los programas de capacitación o la introducción de nuevos recursos de apoyo.

AJUSTE Y MEJORA

- La fase de Ajuste y Mejora es el paso final en la metodología ACTIVA, y se centra en refinar y optimizar las políticas y estrategias basadas en los resultados obtenidos durante la fase de Valoración.

Esta etapa garantiza que la organización pueda adaptarse a las lecciones aprendidas y a las nuevas necesidades que puedan surgir, promoviendo un entorno de mejora continua. A continuación se detallan los pasos clave para realizar ajustes efectivos y cerrar el proceso de implementación:

1. Análisis de Resultados y Retroalimentación:

- Revisión de Resultados: Examina en detalle los resultados de la fase de Valoración, incluyendo encuestas, entrevistas y datos sobre incidentes de seguridad y bienestar. Identifica las áreas que requieren ajustes basados en el feedback recibido y el análisis de impacto.

2. Implementación de Ajustes

- Modificación de Políticas: Realiza los ajustes necesarios en las políticas de seguridad digital y las estrategias psicosociales. Esto puede incluir la actualización de directrices, la mejora de procesos y la introducción de nuevas prácticas.

- Evaluación de Desempeño: Evalúa el desempeño de las políticas y estrategias en función de los objetivos establecidos. Determina si se han alcanzado los resultados esperados y si se han mitigado los riesgos identificados.

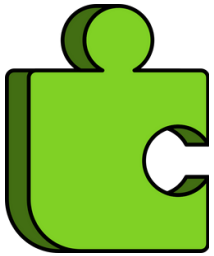
- Optimización de Recursos: Ajusta los recursos y herramientas utilizados para apoyar la seguridad digital y el bienestar psicosocial. Asegúrate de que sean eficaces y accesibles para todos los voluntarios y miembros.

- Refinamiento de Capacitación: Mejora los programas de capacitación basándote en la retroalimentación. Incluye nuevos temas relevantes, ajusta los formatos de las sesiones y asegura que la capacitación sea más efectiva y accesible.

3. Comunicación de Cambios

- Notificación a los Participantes: Informa a los voluntarios y miembros sobre los ajustes realizados y las razones detrás de ellos. Utiliza canales de comunicación adecuados para asegurar que todos estén al tanto de las nuevas directrices y prácticas.

- Actualización de Documentación: Actualiza toda la documentación relacionada con las políticas y estrategias. Asegúrate de que toda la información sea clara y accesible para los voluntarios y miembros.



4. Planificación para la Mejora Continua

- Desarrollo de Nuevos Objetivos: Basado en los ajustes realizados, establece nuevos objetivos para continuar mejorando la seguridad digital y el bienestar psicosocial. Define metas claras y medibles para la siguiente fase del ciclo de mejora continua.

- Integración en el Ciclo de Evaluación: Incorpora los ajustes en el ciclo de evaluación y mejora continua. Asegúrate de que la organización tenga un proceso sistemático para revisar y actualizar las políticas y estrategias de manera regular.

5. Cierre del Proceso

- Revisión Final: Realiza una revisión final del proceso para asegurar que todos los aspectos han sido abordados y que las políticas y estrategias están funcionando como se espera. Documenta las lecciones aprendidas y las mejores prácticas identificadas.

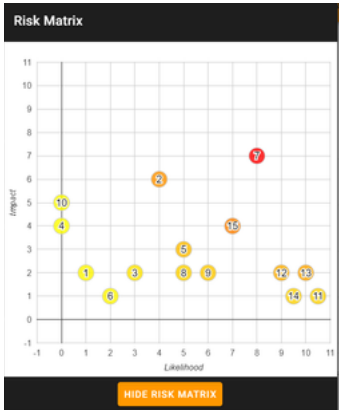
- Celebración de Logros: Reconoce y celebra los logros alcanzados durante el proceso. Agradece a los voluntarios y miembros por su participación y esfuerzo en la implementación de las políticas y estrategias.

- Preparación para el Futuro: Establece un plan para abordar cualquier nuevo riesgo o desafío que pueda surgir. Asegúrate de que la organización esté preparada para adaptarse a futuros cambios y continuar con el proceso de mejora continua.

HERRAMIENTAS - RIESGOS DIGITALES

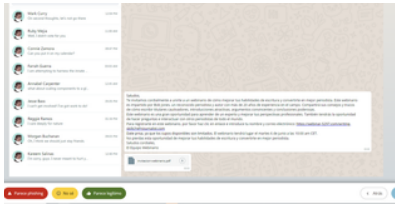
RAWRR

RAWRR (Risk Assessment Workflow for Recommendation Roadmaps) es una aplicación local y multiplataforma que asiste a auditores y otros especialistas de seguridad organizacional, facilitando la recopilación de información y posterior generación de reportes.



Shira.app: Aprende a Identificar el Phishing en un Entorno Seguro

Shira.app es una aplicación educativa diseñada para ayudar a los usuarios a reconocer y evitar ataques de phishing. A través de simulaciones realistas, Shira.app muestra ejemplos de mensajes fraudulentos en diferentes plataformas como correos electrónicos, redes sociales y aplicaciones de mensajería. Los usuarios pueden interactuar con estos escenarios, aprender a detectar señales de alerta y practicar cómo protegerse frente a intentos de phishing.

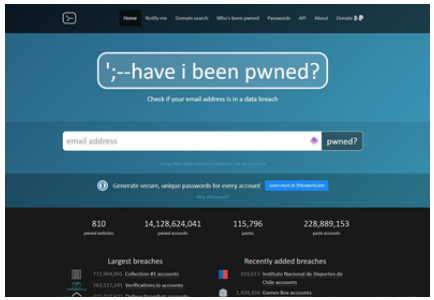


¿Puedes detectar si eres víctima de suplantación de identidad (phishing)?

Identificar la suplantación de identidad (phishing) puede ser más complicado de lo que crees. Phishing es un método en el que un atacante finge ser alguien que conoces para engañarte y obtener tu información personal. para ayudarte a mejorar tu capacidad de detectar estos engaños, utiliza nuestra herramienta interactiva. Descubre si puedes distinguir mensajes falsos y aprende a protegerte mejor. ¡Prueba tu habilidad ahora!

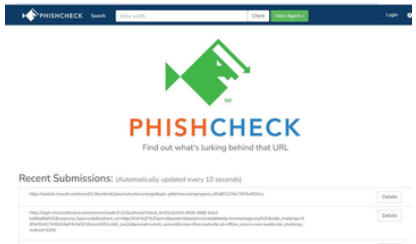
Have I Been Pwned

Descubre si tu información personal ha sido comprometida con Have I Been Pwned. Este sitio web te permite verificar si tu correo electrónico o número de teléfono ha sido expuesto en violaciones de datos conocidas. Simplemente ingresa tu dirección de correo electrónico y revisa si ha aparecido en listas de filtraciones públicas.



¿Es un mensaje phishing?

No te dejes engañar. Con PhishCheck, puedes verificar si un mensaje sospechoso es un intento de phishing antes de hacer clic en cualquier enlace. Simplemente copia y pega la URL o el contenido del mensaje en nuestra herramienta y recibe una evaluación rápida para proteger tu información personal.



REFERENCIAS BIBLIOGRÁFICAS:

- OIT. Enciclopedia de la Seguridad y la salud en el Trabajo. Madrid: Ministerio del Trabajo y Asuntos Sociales; 1998.
- Moreno, B. (2011). Factores y riesgos laborales psicosociales: Conceptualización, historia y cambios actuales. Medicina y Seguridad del Trabajo, 57, 7–9. https://doi.org/10.4321/S0465-546X2011000500002

RECURSOS OFICIALES

https://conexo.org/project/rawrr/

https://shira.app/

https://phishingquiz.withgoogle.com/

https://haveibeenpwned.com/

https://phishcheck.me/

INVENTARIO DE ANSIEDAD DE BECK (BAI)

https://sosvics.eintegra.es/Documentacion/02-Psicosocial/02-03-Documentos_trabajo_prof/02-03-001-ES.pdf

INVENTARIO DE DEPRESIÓN DE BECK (BDI-2)

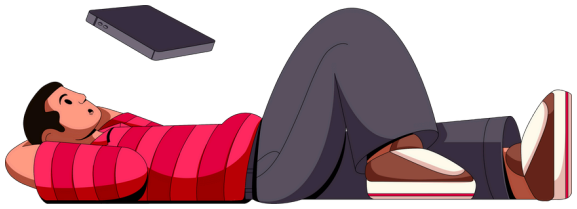
https://www.psi.uba.ar/academica/carrerasdegrado/psicologia/sitios_catedras/obligatorias/070_psicoterapias1/material/inventario_beck.pdf

NOTAS

Conexión Educativa

@ayudaConexionEduEc_bot

https://conexioneducativa.org



Conexión
Educativa