BACK 2 BASICS

SEGURIDAD

MANUAL DE CIBERSEGURIDAD

universidade de aveiro

Co-funded by
the European Union

Cláusula de exención de responsabilidad: 2021-1-PT01-KA220-HED-000023543
El proyecto “Back2Basics” está cofinanciado por la Comisión Europea. Las opiniones y puntos de vista expresados en esta publicación son los de los autores y no reflejan necesariamente los de la Comisión Europea. La Comisión Europea no se hace responsable del uso que pueda hacerse de la información aquí difundida.

BACK 2 BASICS

MANUAL DE CIBERSEGURIDAD

Una guía completa de las mejores prácticas de ciberseguridad de capacita a las personas y organizaciones para protegerse contras las amenazas habituales en el mundo digital.

universidade de aveiro

BIO LIVING

HELLENIC REPUBLIC UNIVERSITY OF MACEDONIA

gri

Título
SEGURIDAD — Manual de ciberseguridad

Proyecto
Back2Basics - Reducir la brecha entre la enseñanza superior y el mercado laboral fomentando las competencias digitales

Referencia del proyecto
Erasmus+ 2021-1-PT01-KA220-HED-000023543

Coordinación
João Rafael Almeida [Oficina de Ciberseguridad de la Universidad de Aveiro]
Cristina Cerqueira [Oficina de Ciberseguridad de la Universidad de Aveiro]
João Paulo Barraca [Oficina de Ciberseguridad de la Universidad de Aveiro]
Rita Santos [Dep. de Comunicación y Arte/Digimedia, Universidad de Aveiro]

Contribuyentes | Socios (por orden alfabético)
Associação Bioliving
GRI — Gabinete de Recolocación Industrial
University of Aveiro
University of Macedonia

Diseño Gráfico
Gonçalo Gomes [Dep. de Comunicación y Arte/ID+, Universidad de Aveiro]

Ilustraciones
Vectorjuice / Freepik

Editorial
UA Editora
University of Aveiro

ISBN
XXX-XXX-XXX-XXX

DOI
XXX-XXX-XXX-XXX

RESUMEN

En un mundo cada vez más interconectado, la ciberseguridad es de vital importancia. Este manual es un buen recurso para las personas y organizaciones que se sumergen en el ámbito de constante evolución de las ciberamenazas. Abarcando temas que van desde la ingeniería social, y el phising hasta la prevención de los softwares maliciosos (malware) y la autenticación multifactor, esta guía proporciona consejos básicos y las mejores prácticas para mitigar los riesgos. Este manual capacita a los lectores para proteger sus activos digitales y mantener una presencia en línea segura, fomentando la concienciación sobre la ciberseguridad, haciendo hincapié en la importancia de las medidas proactivas y ofreciendo orientación sobre el mantenimiento de defensas sólidas. Tanto si eres un particular preocupado por su seguridad personal como si eres una organización que desea mejorar sus protocolos de ciberseguridad, este manual te proporcionará los conocimientos y las herramientas necesarias para navegar por el mundo digital con seguridad y confianza.

BACK 2 BASICS

1 INTRODUCCIÓN

MANUAL DE CIBERSEGURIDAD

INTRODUCCIÓN

En el actual mundo interconectado, en el que la tecnología se ha convertido en parte de nuestra vida cotidiana, no se puede exagerar la importancia de la ciberseguridad. Por ello, fue una de las competencias esenciales del proyecto "Back2Basics - Reducir la brecha entre la enseñanza superior y el mercado laboral fomentando las competencias digitales", Erasmus + (2021-1-PT01-KA220-HED- 000023543), que tiene como objetivo abordar la transformación digital en el sistema de educación superior y acercar estos sistemas al mercado laboral, trabajando en la mejora de las competencias digitales.

Este exhaustivo manual está diseñado para proporcionar a los usuarios los conocimientos fundamentales necesarios para navegar por el panorama de las ciberamenazas, en constante evolución, y protegerse de los posibles riesgos. Aunque la era digital ha aportado enormes beneficios, también ha expuesto nuestra información a una amplia gama de problemas potenciales que pueden tener graves consecuencias.

Al comprender estas cuestiones, las personas pueden reconocer mejor la importancia de la ciberseguridad en su vida personal y profesional.

El aumento insidioso de los ataques de ingeniería social pone de manifiesto la creciente sofisticación de los ciberdelincuentes, que emplean tácticas psicológicas para manipular a personas desprevenidas para que divulguen información confidencial o realicen acciones que comprometen su seguridad. El phishing consiste en correos electrónicos o sitios web fraudulentos diseñados para engañar a los usuarios y hacerles compartir información personal, como contraseñas o datos de tarjetas de crédito. Ser víctima de este tipo de ataques puede provocar pérdidas económicas, robos de identidad y daños a la reputación. Además, la prevalencia del malware supone una amenaza significativa tanto para los particulares como para las organizaciones. El malware es software diseñado con fines maliciosos.

Este tipo de software puede infectar ordenadores o redes y comprometer la seguridad de los datos y la integridad del sistema. Por ejemplo, el ransomware es un tipo de malware que cifra archivos valiosos en la máquina objetivo y exige un rescate por su liberación. Organizaciones de todos los tamaños han sido víctimas de este tipo de ataques, que han provocado pérdidas financieras, operaciones interrumpidas y daños a su reputación.

Uno de los principales objetivos de este manual es concienciar al público en general sobre la importancia de la ciberseguridad. Profundizará en diversos temas, como la ingeniería social, el phishing, la prevención del malware, la gestión de contraseñas, la autenticación multifactor y otros. Proporcionará consejos prácticos, mejores prácticas y ejemplos del mundo real para que los lectores puedan salvaguardar su vida digital y mitigar los riesgos asociados a las ciberamenazas. En los siguientes capítulos, se explorarán algunas de las medidas y estrategias proactivas que pueden emplearse para mantenerse seguro en el mundo digital. Mediante el desarrollo de una base sólida de concienciación sobre ciberseguridad y la adopción de prácticas defensivas eficaces, las personas pueden construir colectivamente un entorno digital más seguro y resistente para todos.

BACK 2 BASICS

2

MANUAL DE CIBERSEGURIDAD

AMENAZAS COMUNES

AMENAZAS COMUNES

El contexto de una amenaza en ciberseguridad debe verse como un precursor de un incidente no deseado que puede resultar en daños a datos, sistemas, individuos u organizaciones. Esta sección proporciona una visión general de las amenazas comunes para las personas.

INGENIERÍA SOCIAL

La ingeniería social va más allá de una táctica engañosa utilizada por los ciberdelincuentes para manipular a las personas con el fin de que revelen información sensible o realicen acciones que puedan comprometer su seguridad. Esta técnica no se limita al ciberespacio y puede darse fuera de él, con el objetivo de recabar información privilegiada sobre un sistema específico, que puede ayudar a los atacantes a tener éxito. Aprovecha la psicología humana y explota nuestras tendencias inherentes,

como la confianza, la curiosidad o el deseo de ayudar a los demás. ¿Por qué en importante?

La ingeniería social pretende inducir a las personas a tomar decisiones sin pensar demasiado en lo que ocurre, lo que puede resultar ventajoso para los atacantes que explotan las vulnerabilidades de esos procesos. En definitiva, el objetivo principal es obligar a un individuo a llevar a cabo una acción específica sin pensarlo detenidamente. Cuando más reflexionen las personas sobre las acciones que estén realizando, más probabilidades tendrán de reconocer que estas acciones forman parte de una manipulación.

Pensemos, por ejemplo, en un anuncio de televisión de una artista famosa. El anuncio comienza en un entorno sombrío con una canción lúgubre, que retrata a la artista en medio de un ambiente deprimente. La escena cambia a otro lugar en el que unos cachorros aparecen angustiados y desnutridos, evocando una sensación de desesperación. La artista explica que sin nuestras donaciones los cachorros no sobrevivirán. Tras estas conmovedoras escenas, el artista reaparece, ahora alegre y rodeado de cachorros sanos acompañados de una entusiasta canción. ¿Cuál es el mensaje subyacente? El anuncio sugiere que, por un pequeño donativo, la difícil situación de estos pobres animales puede transformarse y ellos pueden compartir su amor con el público. Aunque la intención puede no ser egoísta, este anuncio pretende manipular las emociones del público, provocando sentimientos positivos cuando la gente contribuye a salvar a los cachorros.

El mismo principio puede aplicarse con fines maliciosos. En una situación hipotética en la que un atacante quiere acceder a una empresa concreta, este individuo puede manipular la atención de la recepcionista para saltarse la primera barrera humana. Un ejemplo de este tipo de estrategias podría ser crear una sensación de urgencia, por ejemplo, alegando una necesidad urgente de mantenimiento en una parte específica del edificio. Aunque este ejemplo pueda parecer trivial, es importante reconocer que la ingeniería social no se limita al ciberespacio.

Los ciberdelincuentes diseñan meticulosamente sus ataques para que parezcan legítimos, explotando vulnerabilidades humanas comunes para lograr sus objetivos maliciosos. En el ciberespacio, estos ataques pueden adoptar diversas formas, como el phishing, el pretexto, el señuelo o incluso la manipulación física. El éxito de los ataques de ingeniería social se basa a menudo en crear una sensación de urgencia, explotar la con-

fianza o aprovechar los desencadenantes emocionales. Por ejemplo, un atacante puede redactar un correo electrónico haciéndose pasar por un representante bancario, alegando que la cuenta del destinatario se ha visto comprometida e instándole a hacer click en un enlace para resolver el problema. Estas tácticas manipulan a las personas para que actúen sin evaluar críticamente la situación.

Para protegerse contra los ataques de ingeniería social, las personas deben permanecer atentas y desarrollar un sano escepticismo al participar en cualquier forma de comunicación. Es esencial verificar la autenticidad de las solicitudes, sobre todo si implican información sensible o acciones inesperadas. Esta verificación puede lograrse poniéndose en contacto de forma independiente con la organización o persona a través de un canal de comunicación de confianza para confirmar la legitimidad de la solicitud. Adoptando un enfoque prudente y manteniéndose informados sobre las últimas técnicas de ingeniería social, los individuos pueden mejorar su capacidad de protegerse contra estas tácticas engañosas.

PHISHING, VISHING Y SMISHING

Una forma común de ingeniería social es el phishing, en el que los atacantes envían correos electrónicos fraudulentos que parecen proceder de organizaciones o personas de confianza. Estos mensajes suelen contener peticiones urgentes, ofertas tentadoras o alertas inquietantes, con el objetivo de incitar a los destinatarios a actuar de inmediato. Pueden solicitar información confidencial, como contraseñas, números de tarjetas de crédito o credenciales de inicio de sesión, bajo el pretexto

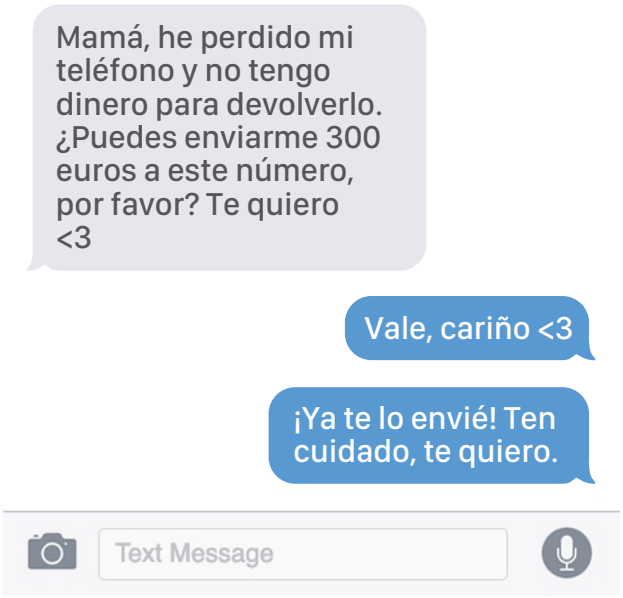
de una necesidad legítima. Estos ataques se manifiestan de diversas formas, como el phishing por correo electrónico, el smishing (phishing por SMS) y el phishing por voz (vishing). El phishing por correo electrónico es el más común, ya que los atacantes envían correos electrónicos que parecen auténticos, a menudo utilizando logotipos oficiales, lenguaje y elementos de diseño para engañar a los destinatarios. El smishing y el vishing emplean tácticas similares, pero a través de mensajes de texto o llamadas telefónicas, respectivamente.

El objetivo de estos ataques puede desglosarse en varias finalidades:

- **Entregar cargas útiles maliciosas -la parte de un software malicioso que ejecuta acciones maliciosas- que proporcionan acceso remoto a los atacantes;**
- **Robar las credenciales de la víctima;**
- **Recopilar otra información que pueda utilizarse para escalar otro ataque.**

Además de estos mensajes genéricos que llegan a un público amplio, existe una técnica más personalizada conocida como spear phishing. Este método requiere cierta preparación por parte de los atacantes, ya que necesitan obtener información sobre la víctima. Normalmente, utilizan algo muy personal que está disponible públicamente en línea y es fácilmente accesible para cualquiera. Esta información suele proceder de publicaciones en redes sociales, a veces publicadas involuntariamente por los familiares de la víctima, entre otros.

Pensemos, por ejemplo, en un grupo de amigos que se va de vacaciones durante una semana. Durante este viaje, es normal publicar varias fotos en diversas redes sociales. Si un atacante vigila a este grupo en línea y posee información adicional sobre sus familiares, puede utilizar este conocimiento para ponerse en contacto con los padres de uno de los amigos. En este punto, el atacante podría utilizar un teléfono o perfil ficticio para iniciar el contacto con el siguiente contexto:



La acción esperada por parte de los padres sería realizar una doble comprobación antes de enviar dinero. Sin embargo, ciertos elementos de la historia tenían sentido, creando un escenario perfecto para caer víctima del spear phishing. Nuestra vida cotidiana está llena de ejemplos similares, casos en los que las personas actúan de forma impulsiva sin pensar detenidamente.

Para evitar ser víctima de ataques de phishing, es esencial mantenerse alerta y adoptar medidas preventivas. En el caso de los correos electrónicos, lo primero que hay que hacer es examinar la dirección de correo electrónico del remitente, prestando atención a cualquier discrepancia o dominio desconocido que no coincida con la supuesta organización. A continuación, hay que evaluar el contenido del correo electrónico, prestando atención a errores ortográficos o gramaticales, saludos genéricos o solicitudes urgentes diseñadas para crear una sensación de pánico. Las organizaciones legítimas suelen dirigirse a las

personas por su nombre y proporcionar información clara y concisa. Por último, se deben evitar hacer clic en enlaces sospechosos o descargar archivos adjuntos sin verificar su legitimidad. La incorporación de estas prácticas aumentará la resistencia personal frente a estas estafas. Una estrategia para identificar los enlaces maliciosos consiste en pasar el ratón por encima del enlace para descubrir su destino real y asegurarse de que conducen a sitios web legítimos. Las personas deben tener cuidado si el enlace redirige a una URL desconocida. Además, se aconseja escribir las URL directamente en el navegador o utilizar marcadores para acceder a sitios web de confianza.

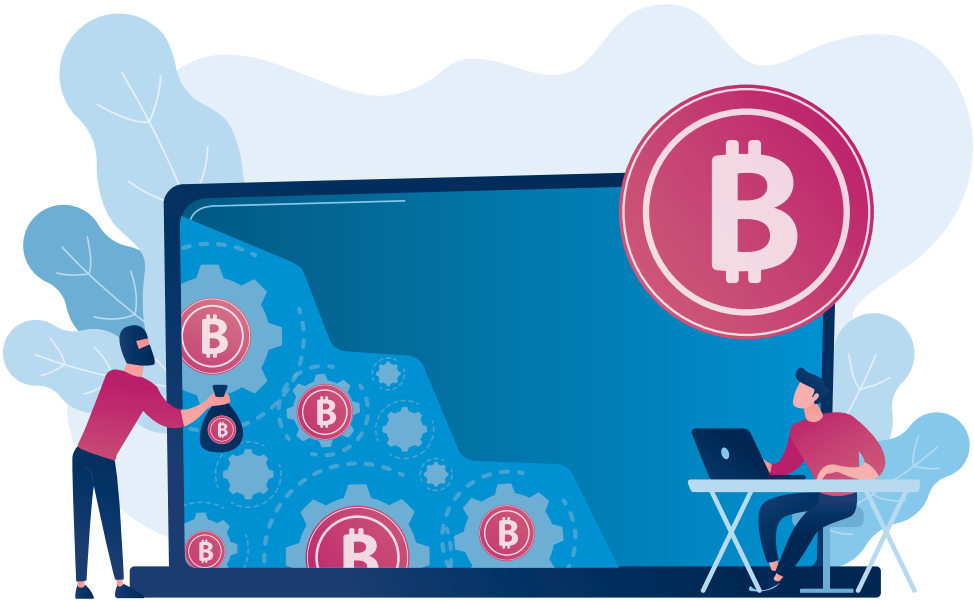
Además, hay que instalar y actualizar regularmente software de seguridad acreditado, como programas antivirus o antimalware, para detectar y bloquear posibles intentos de phishing. Educarse sobre las técnicas de phishing también es crucial para reconocer y evitar estos ataques, además de estar informado sobre las últimas tendencias de phishing, las señales de alarma más comunes y las nuevas tácticas empleadas por los ciberdelincuentes.

LOS INVASORES SILENCIOSOS: UNA VISIÓN GENERAL DE LOS TIPOS DE MALWARE

El malware hace referencia a cualquier software diseñado específicamente para dañar o explotar sistemas informáticos, redes o individuos. Incluye una amplia gama de programas maliciosos, como virus, gusano informático, troyanos, programas espía y ransomware. El malware puede distribuirse a través de diversos medios, como correos electrónicos infectados, sitios web comprometidos o descargas maliciosas. Una vez instalado, el malware puede poner en peligro los datos, robar información personal, interrumpir el funcionamiento del sistema o proporcionar acceso no autorizado a los ciberdelincuentes. Comprender los distintos tipos de malware es crucial para crear estrategias de defensa eficaces.

A continuación, describimos brevemente las distintas categorías de malware:

- **Virus:** Estos parásitos digitales se infiltran en los archivos anfitriones, propaganda su código cuando se ejecuta el archivo infectado. Al igual que los virus biológicos, los virus informáticos se replican, causado daños y caos a su paso.
- **Gusano informático:** A diferencia de los virus, los "gusanos" funcionan de forma independiente y se propagan por las redes, aprovechando las vulnerabilidades para propagarse. Su naturaleza autorreplicante les permite infectar rápidamente múltiples sistemas.
- **Troyanos:** Llamados así por el legendario engaño griego, los troyanos se hacen pasar por software legítimo, engañando a los usuarios para que los inviten a entrar. Una vez dentro, allanan el camino para el acceso y control no autorizados.
- **Programas espía:** Operan en la sombra, recopilan en silencio información confidencial, desde contraseñas hasta datos personales, a menudo con fines de espionaje o robo de identidad.



- **Adware:** Aunque menos siniestro, el adware bombardea a los usuarios con anuncios no deseados, afectando al rendimiento del sistema y a la experiencia del usuario. A menudo sirve como vehículo para generar ingresos para los ciberdelincuentes.• Rootkits: Sigilosos y escurridizos, los rootkits profundizan en el núcleo de un sistema, proporcionando acceso y control persistentes a los actores maliciosos. Son muy difíciles de detectar y eliminar.

- **Keyloggers:** Estas herramientas subrepticias rastrean y registran las pulsaciones del teclado, capturando información sensible como contraseñas y datos de tarjetas de crédito, lo que permite a los ciberdelincuentes robar datos valiosos.

- **Ransomware:** Se trata de un tipo específico de malware que cifra los archivos de la víctima, dejándolos inaccesibles hasta que se paga un rescate. Normalmente, se infiltra en los sistemas a través de correos electrónicos de phishing, archivos adjuntos maliciosos o kits de exploits. Una vez activado, el ransomware cifra los archivos importantes y muestra una nota de rescate exigiendo el pago a cambio de la clave de descifrado. Los ataques de ransomware son cada vez más sofisticados y se dirigen a particulares, empresas e incluso infraestructuras críticas.

En el pasado, el malware se elaboraba con cierta vulnerabilidad, lo que ayudaba a los profesionales de la ciberseguridad a revertir los daños causados. Sin embargo, en los últimos tiempos, los ciberdelincuentes han mejorado la "calidad" de sus aplicaciones utilizando algoritmos conocidos por su gran resistencia al descifrado. Esto crea un escenario especialmente difícil, ya que en un ordenador común se tardarían miles de millones, o incluso billones, de años en recuperar la clave para descifrar los archivos. Aunque pagar el rescate pueda parecer razonable, sobre todo si se tiene en cuenta el impacto de la información perdida, suele ser la peor decisión por varias razones. En primer lugar, la persona que paga el rescate indica indirectamente al atacante que es un objetivo excelente porque el pago está garantizado. En otras palabras, es como fijar un

objetivo cibernético en esa persona. En segundo lugar, y no menos importante, está la incertidumbre de que la clave proporcionada descifre los archivos. ¿Quién puede garantizar que el atacante actuará honestamente?

El impacto del malware va más allá de los sistemas indivi-duales y se extiende a los ámbitos personal, empresarial y gubernamental.

- **Pérdidas económicas:** Los incidentes relacionados con el malware pueden dar lugar a pérdidas financieras sustanciales, incluyendo el pago de rescates, costes de recuperación y posibles sanciones legales.
- **Fuga de datos:** El malware compromete datos sensibles, poniendo en peligro la privacidad personal y la confidencialidad corporativa. Las secuelas de las filtraciones de datos pueden ser duraderas e irreparables.
- **Interrupción de las operaciones:** Los ataques de ransomware pueden paralizar las operaciones, provocando tiempos de inactividad y afectando a la productividad a gran escala.
- **Daño de la reputación:** Las organizaciones afectadas por incidentes de malware suelen sufrir daños en su reputación, lo que erosiona la confianza de los clientes.
- **Preocupación por la seguridad nacional:** Las campañas de malware patrocinadas por el Estado plantean importantes problemas de seguridad nacional, ya que se dirigen contra infraestructuras críticas e instituciones gubernamentales.

En el vasto e intrincado panorama de la ciberseguridad, el malware emerge como un adversario formidable. Sus diversas formas y su impacto insidioso nos recuerdan constantemente las amenazas digitales a las que nos enfrentamos en nuestro mundo interconectado. Al comprender la naturaleza polifacética del malware, podemos entender mejor la necesidad de medidas de ciberseguridad sólidas y de una vigilancia continua.

A medida que la tecnología sigue evolucionando, la lucha contra el malware sigue siendo un aspecto fundamental para salvaguardar nuestro futuro digital.

DESENMASCARAR SITIOS WEB ENGAÑOSOS Y NOTICIAS FALSAS

En una era caracterizada por la accesibilidad sin precedentes a la información, ha surgido un siniestro trasfondo en el panorama digital: los sitios web engañosos y la difusión generalizada de noticias falsas. A medida que nos adentramos en los intrincados caminos de la red, resulta cada vez más crucial

navegar con cautela por estas aguas traicioneras. Profundizando en el mundo de los sitios web engañosos y descubriendo los inquietantes efectos de las noticias falsas, podemos describir puntos clave sobre su procedencia, su funcionamiento y sus amplias repercusiones.

En el mundo de los sitios engañosos, la ilusión de legitimidad se teje hábilmente a través de ciertas tácticas. Estas plataformas engañosas, utilizan a menudo un diseño sofisticado y la imitación para emular fuentes reales, difuminando las líneas entre lo real y el engaño. La manipulación sutil entra en juego, aprovechando el lenguaje persuasivo y las imágenes engañosas para explotar los prejuicios cognitivos, incitando a los usuarios a consumir y compartir contenidos sin pensárselo dos veces. La autoridad fingida aumenta aún más la ilusión, ya que los sitios web engañosos fabrican avales y testimonios, creando un aspecto externo de credibilidad que atrapa fácilmente a los lectores desprevenidos. Dentro de esta intrincada red de engaño, surge un próspero ecosistema de información falsificada. Estas plataformas presentan hábilmente una mezcla de datos auténticos e inventados, lo que da lugar a una distorsión de la realidad que siembra la confusión entre un público desprevenido.

Con una intención maliciosa en su origen, la difusión de noticias falsas a menudo funciona como una herramienta para engañar, manipular o influir en la opinión pública con el fin de promover programas o ideologías específicos.

Impulsada por catalizadores tecnológicos, la rápida difusión de noticias falsas se intensifica a través de la viralidad de las redes sociales y la amplificación algorítmica. Esta dinámica permite que la desinformación penetre en la audiencia en plazos sin precedentes. El efecto corrosivo se extiende a la erosión de la confianza, ya que la exposición repetida a noticias falsas ero-

siona la confianza del público en las instituciones establecidas, cultivando una atmósfera de escepticismo que podría disminuir la credibilidad de la información objetiva. La influencia de las noticias falsas no se detiene ahí, sino que se extiende a las creencias individuales y a los procesos colectivos de toma de decisiones, lo que subraya la urgencia de contrarrestar su insidioso impacto.

BACK 2 BASICS

3

MANUAL DE CIBERSEGURIDAD

CIBERHIGIENE: BUENAS PRÁCTICAS

CIBERHIGIENE: BUENAS PRÁCTICAS

En el mundo digital actual, en el que nuestras vidas están entrelazadas con la tecnología de una forma sin precedentes, el concepto de ciberhigiene ha surgido como piedra angular de un comportamiento en línea responsable y seguro. Al igual que damos prioridad a la higiene personal para mantener nuestro bienestar físico, adoptar prácticas sólidas de ciberhigiene es esencial para preservar nuestra salud digital y protegernos contra un panorama de ciberamenazas en rápida evolución. Esta sección del manual, profundiza en el ámbito de la ciberhigiene, destacando las buenas prácticas que permiten a las personas navegar por el ámbito digital con confianza, resistencia y una mayor conciencia del panorama de la ciberseguridad. Desde el refuerzo de las contraseñas hasta el cultivo de un ojo perspicaz para los intentos de suplantación de identidad, este capítulo sirve como guía para elevar su bienestar digital y fomentar una experiencia en línea más segura.

DEFINICIÓN DE CIBERHIGIENE

En un mundo cada vez más interconectado, en el que nuestras vidas están entrelazadas con la tecnología, es esencial dar prioridad a la ciberseguridad. Al igual que practicamos la higiene personal para proteger nuestro bienestar físico, adoptar buenos hábitos de ciberhigiene es crucial para salvaguardar nuestra vida digital. Pero, ¿qué es exactamente la ciberhigiene?

La ciberhigiene se refiere a un conjunto de buenas prácticas y hábitos que las personas y las organizaciones deben adoptar para garantizar la seguridad e integridad de su entorno digital. Abarca una amplia gama de acciones y comportamientos que contribuyen a prevenir las ciberamenazas, como las infecciones por malware, las vulneraciones de datos y el robo de identidad.

Ser ciberhigiénico es muy importante en el panorama digital actual. Las ciberamenazas siguen evolucionando y sofisticándose, lo que plantea riesgos significativos, tanto para las personas y organizaciones. Practicando una buena ciberhigiene, podemos protegernos proactivamente a nosotros mismos y a nuestra información sensible de los actores maliciosos. Esto ayuda a prevenir consecuencias potenciales como el robo de identidad, las pérdidas financieras y el daño a la reputación. Mantener contraseñas seguras, actualizar regularmente el software y ser cauteloso ante los intentos de phishing son sólo algunos ejemplos de prácticas de ciberhigiene que pueden reducir significativamente la probabilidad de ser víctima de ciberataques. Además, ser ciberhigiénico no sólo protege nuestro propio bienestar digital, sino que también contribuye a la seguridad colectiva del mundo interconectado, creando un entorno en línea más seguro para todos.

RECOMENDACIONES PARA ESTAR SEGURO EN INTERNET

Actualizar regularmente el software es como cuidar un jardín digital. Los sistemas operativos, las aplicaciones y el software de seguridad evolucionan para hacer frente a las nuevas vulnerabilidades y mejorar la protección. Un sistema actualizado es su primera línea de defensa contra las ciberamenazas, ya que

garantiza el cierre hermético de los posibles puntos de entrada de los piratas informáticos. Al activar las actualizaciones automáticas o comprueba constantemente si hay actualizaciones, se frustrarán los intentos de los ciberdelincuentes de explotar el software obsoleto y protegerá su jardín digital. Adoptar la práctica de las actualizaciones de software es un poderoso paso hacia una existencia digital más segura. Con cada actualización, dota a sus dispositivos de los últimos parches de seguridad, lo que hace exponencialmente más difícil que los ciberatacantes vulneren sus defensas. Estas actualizaciones no sólo repelen las amenazas inminentes, sino que cultivan una mentalidad proactiva que refuerza la resistencia de tu ciberseguridad. Al dedicar unos minutos a las actualizaciones periódicas, contribuyes a un entorno en línea más seguro para ti y para los demás, demostrando la potencia de la vigilancia colectiva.

En el ámbito de la ciberseguridad, una contraseña sólida es la fortaleza virtual del usuario, que protege de accesos no autorizados. Crear una contraseña segura no es una mera tarea, es un arte. Entrelazando letras, números, símbolo y mayúsculas, es posible componer una contraseña formidable y difícil de descifrar.

Cada cuenta merece su propia contraseña. Considera la posibilidad de recurrir a la ayuda de un gestor de contraseñas fiable, que libere a los usuarios de la carga mental que supone recordar códigos intrincados y garantice que tus claves digitales permanecen almacenadas de forma segura. En las secciones siguientes se ofrecen más detalles sobre este tema

En medio de las corrientes digitales, las estafas de phishing son los remolinos engañosos que buscan atrapar a víctimas desprevenidas. La vigilancia es su brújula; antes de sucumbir al señuelo tentador de un correo electrónico, analiza su autentici-

dad. Pasar el ratón por encima de los enlaces para discernir su verdadero destino es un acto pequeño pero potente que puede salvaguardarle del precipicio de una posible vulneración. Cuando un correo electrónico parezca urgente, haz una pausa y actúa con cautela. Este es el modus operandi de los ciberestafadores que tratan de sacar provecho de las decisiones precipitadas. Confía en tus instintos y verifica la identidad del remitente, disuadiendo así el truco de una operación de phishing.

El escepticismo, junto con el pensamiento crítico, forman un escudo indomable contra la marea traicionera de intentos de phishing. Piensa en ti mismo como un ciberdetective que investiga pistas y reconstruye la verdad. Al adoptar una mentalidad vigilante y cautelosa en línea, te transformas en un navegante experto que surca las traicioneras aguas del engaño con un criterio implacable. Recuerda que un momento de escepticismo puede evitar horas de control de daños, lo que demuestra la potencia de una mentalidad vigilante y crítica.

Las redes Wi-Fi públicas ofrecen el atractivo de una conectividad sin fisuras, pero a menudo esconden riesgos ocultos. El uso de estas redes exige un enfoque cauteloso; trátelas como mercados abarrotados en los que se expone información personal. Las actividades con datos sensibles, como la banca electrónica o la transferencia de documentos confidenciales, deben reservarse para conexiones seguras y privadas. El uso prudente de una Red Privada Virtual (VPN) actúa como un manto digital, encriptando tus datos y protegiéndolos de miradas indiscretas, haciéndote inmune a posibles fisgones. En el ámbito de la seguridad en la red, la conciencia y la prudencia son las principales guías. Considera las redes Wi-Fi públicas como plazas llenas de extraños, donde cualquier transeúnte podría escuchar tus secretos. La máscara digital de una VPN, añade una capa adicional de protección, asegurando que tu huella digital permanezca oculta a los curiosos. Adoptando estas medidas, dispondrás de las herramientas necesarias para recorrer el mundo virtual con confianza, sabiendo que tus actividades en línea están protegidas frente a posibles adversarios.

Aunque estas estrategias contribuyen a aumentar la seguridad en línea, vamos a profundizar en una lista de las diez mejores prácticas para fomentar la resiliencia frente a las ciberamenazas.

1. **Contraseñas seguras:** Crea contraseñas únicas y fuertes para cada cuenta.
2. **Autenticación multifactor (AMF):** Usa AMF siempre que esté disponible.
3. **Actualizaciones periódicas:** Mantén el software y los dispositivos actualizados.
4. **Sé precavido en Internet:** Estate atengo a los correos electrónicos y enlaces sospechosos.
5. **Evita las redes Wi-Fi públicas:** Evita las actividades sensibles en las redes Wi-Fi públicas.
6. **Copias de seguridad:** Haz copias de seguridad periódicas de archivos importantes.
7. **Ajustes de privacidad:** Ajusta la privacidad de las redes sociales.
8. **Asegura los dispositivos:** Bloquea los dispositivos con contraseñas fuertes.
9. **Piensa antes de hacer click:** Sé precavido con las descargas y los enlaces.
10. **Mantente informado:** Mantente informado sobre las amenazas de ciberseguridad.

MITIGACIÓN Y RECUPERACIÓN

Los ciberataques se han convertido en una forma prevalente y sofisticada de ciberdelincuencia, causando importantes daños a organizaciones de todo el mundo. Para minimizar su impacto y recuperarse eficazmente de este tipo de incidentes, es crucial seguir una serie de directrices bien definidas. Algunas de las mejores prácticas para implementar una sólida estrategia de copias de seguridad para proteger sus valiosos datos pueden ser las siguientes:

- **Aislamiento inmediato:** El primer paso para contener un ataque, por ejemplo, de ransomware, es desconectar todos los dispositivos infectados, como ordenadores, portátiles o tabletas, de cualquier conexión de red, ya sea por cable, inalámbrica o móvil. En casos graves, considere la posibilidad de apagar el Wi-Fi, desactivar las conexiones de red principales y desconectarse de Internet si es necesario.

- **Restablece las credenciales:** Restablecer las credenciales, especialmente las contraseñas de las cuentas de administrador y de sistema, es crucial para evitar nuevos accesos no autorizados. Sin embargo, hay que tener cuidado para no bloquear los sistemas esenciales necesarios para la recuperación.

- **Borra de forma segura los dispositivos infectados:** En el caso de ataques de malware, para erradicar el problema por completo borre de forma segura los dispositivos infectados y reinstale el sistema operativo. Este paso garantiza la eliminación de cualquier resto de malware y deja el sistema limpio para la recuperación.

- **Verifica la integridad de la copia de seguridad:** Antes de restaurar a partir de una copia de seguridad, asegúrate de que está libre de cualquier tipo de malware. Realiza la restauración sólo si estás seguro de que tanto la copia de seguridad como el dispositivo en el que la instalas están limpio.

- **Conéctate a una red limpia:** Para descargar, instalar y actualizar el sistema operativo y el resto del software, conecta los dispositivos a una red limpia. Esto garantiza que no se transfieran por error archivos infectados durante el proceso de recuperación.

- **Instala y actualiza un software antivirus:** Protege tus sistemas de futuros ataques instalando, actualizando y ejecutando un software antivirus fiable. Escanear regularmente sus dispositivos con las últimas definiciones antivirus puede ayudar a identificar y eliminar cualquier infección restante.

- **Reconexión a la red:** Una vez que hayas tomado las precauciones necesarias y garantizado la integridad de tus sistemas, vuelve a conectarte a tu red. No obstante, vigila de cerca el tráfico de red y realiza análisis antivirus periódicos para detectar cualquier signo de malware persistente.

DISEÑO DE UNA ESTRATEGIA SÓLIDA DE COPIAS DE SEGURIDAD

La mejor solución para mejorar la seguridad en el ciberespacio es anticiparse a los posibles problemas. Para estar preparado frente a las ciberamenazas, se recomienda utilizar copias de seguridad, concretamente aplicando una sólida política de copias de seguridad que haga hincapié en la realización de copias periódicas de los archivos críticos. La importancia de estos archivos puede variar para cada usuario u organización, por lo que es esencial evaluar y priorizar tus necesidades específicas. Las recomendaciones son las siguientes:

- **Copias de seguridad en línea y fuera de ella:** Para proteger tus copias de seguridad de los ataques, almacenadlas en una ubicación diferente, fuera del sistema. Considera el uso de servicios de almacenamiento en la nube diseñados para copias de seguridad

seguras. Diversifica las soluciones de copia de seguridad y las ubicaciones de almacenamiento para minimizar el riesgo de pérdida de datos. La adhesión a la estrategia de copia de seguridad 3-2-1 garantiza la redundancia y la resistencia.

- **Desconecta los dispositivos de copia de seguridad:** Evita mantener conectados permanentemente a tu red discos duros externos que contengan copias de seguridad. En caso de ataque, si estos dispositivos están conectados, pueden verse afectados. Los operadores de ransomware suelen atacar a los dispositivos de copia de seguridad conectados, lo que dificulta la recuperación de los datos. Desconectarlos cuando no se utilizan mitiga este riesgo.

- **Protege las versiones anteriores:** Asegúrate de que el proveedor de servicios en la nube que has elegido protege las versiones anteriores de las copias de seguridad. Algunos servicios sincronizan automáticamente los archivos, sustituyendo potencialmente las versiones no cifradas por copias cifradas. Mantener varias versiones de las copias de seguridad garantiza la disponibilidad de datos no corruptos para su recuperación.

- **Revisa los sistemas de seguridad:** Revisa regularmente los servidores de copia de seguridad para solucionar cualquier vulnerabilidad que puedan aprovechar los atacantes. Identificar y corregir los puntos débiles puede mejorar la seguridad y resistencia de las copias de seguridad.

- **Verifica que los dispositivos estén limpios:** Antes de iniciar el proceso de restauración, asegúrate de que tus copias de seguridad sólo están conectadas a dispositivos limpios conocidos. Además, analiza las soluciones de copia de seguridad en busca de malware para evitar reintroducir inadvertidamente archivos infectados en tu red.

Siguiendo las pautas recomendadas y aplicando una estrategia de copia de seguridad sólida, puedes minimizar significativamente el impacto de un brote de ransomware y garantizar un proceso de recuperación rápido y eficaz. Actualizar y probar

periódicamente las copias de seguridad y los procedimientos de recuperación de datos es crucial para garantizar que, en caso de ciberataque, se recuperen eficazmente los datos y se minimice el tiempo de inactividad.

BACK 2 BASICS

4

MANUAL DE CIBERSEGURIDAD

GESTIÓN Y AUTOPROTECCIÓN DE CONTRASEÑAS

GESTIÓN Y AUTOPROTECCIÓN DE CONTRASEÑAS

La gestión eficaz de contraseñas es un aspecto fundamental de la autoprotección en el panorama digital. Abarca no sólo la creación de contraseñas fuertes y únicas, sino también su gestión diligente y su revisión periódica. Esto implica emplear estrategias, como utilizar un gestor de contraseñas fiable para almacenar y organizar las distintas contraseñas, asegurándose de que cada cuenta tenga una contraseña distinta para evitar que una brecha en una cuenta comprometa otras cuentas. También es crucial actualizar periódicamente las contraseñas, sobre todo las de cuentas sensibles, y estar alerta ante posibles ataques de phishing. La autoprotección se extiende al conocimiento de las funciones de seguridad que ofrecen las distintas plataformas, como la autenticación de dos factores, que añade una capa adicional de seguridad. Igualmente, importante es ser consciente de la huella digital de cada uno y de los riesgos potenciales que conlleva compartir información personal en línea. Manteniéndose informados y adoptando prácticas

sólidas de gestión de contraseñas, los usuarios pueden mejorar significativamente su seguridad en línea y proteger su información personal y confidencial de accesos no autorizados.

RIESGOS DE LAS CONTRASEÑAS POCO SEGURAS

Antes de definir qué son las contraseñas débiles y el impacto de su debilidad, primero tenemos que entender cómo los atacantes pueden descifrar nuestras credenciales. Existen diferentes formas de obtener las credenciales de un individuo, suponiendo que éstas no hayan sido proporcionadas en un ataque de phishing. Un atacante puede interceptar la comunicación, realizando lo que se conoce como un ataque Man-In-the-Middle Con la popularización de las comunicaciones HTTPS, estos ataques se han vuelto menos efectivos, por lo que no los discutiremos más en este documento. Sin embargo, otra técnica consiste en robar bases de datos explotando las vulnerabilidades existentes en las aplicaciones web.

Este último problema sigue siendo preocupante y es complejo de controlar. Cuando un atacante consigue robar una base de datos privada que contiene credenciales, éstas se almacenan de tres formas:

1. **Como texto libre (menos común en la actualidad);**
2. **Utilizando un hash, que es una técnica que convierte la contraseña en algo diferentes utilizando algoritmos irreversibles; y**
3. **Utilizando un hash con sal, que es más robusto.**

El proceso de hash de una contraseña se basa en funciones de recopilación. El objetivo de estas funciones es la creación de un conjunto definido de bits que representen la información original. Éstas siguen algunos principios, uno de los cuales define que utilizando un hash no debe ser posible obtener la información original que creó dicho hash.

Por lo tanto, un atacante que disponga del hash de una contraseña no podrá obtenerla directamente.

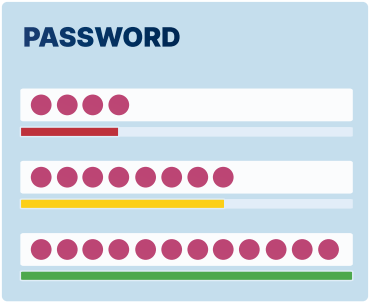
Los hashes iniciales se diseñaron para ser seguros, pero descubrimientos posteriores revelaron ciertas técnicas capaces de romper algunos hashes casi instantáneamente. Esto llevó al

desarrollo de algoritmos hash más avanzados y seguros. La vulnerabilidad de las contraseñas queda expuesta con mayor frecuencia en escenarios como:

- **Almacenadas en bases de datos comprometidas:** Cuando las contraseñas se almacenan en bases de datos no protegidas adecuadamente, se vuelven susceptibles de acceso no autorizado y posibles vulneraciones.
- **Almacenadas en texto claro:** Almacenar las contraseñas en texto claro, sin ningún tipo de cifrado, las convierte en objetivos fáciles para los ciberdelincuentes.
- **Representadas mediante hashes:** Aunque los hashes se utilizan

para mayor seguridad, se ha descubierto que ciertos algoritmos de hashing son vulnerables, lo que hace que las contraseñas sean susceptibles de ataques.

- **Interceptadas en la comunicación:** Las contraseñas pueden ser interceptadas durante su transmisión a través de redes, especialmente si el canal de comunicación no está cifrado de forma segura.
- **Redes desprotegidas:** El uso de contraseñas en redes desprotegidas o públicas aumenta el riesgo de que sean capturadas por agentes maliciosos, ya que estas redes suelen carecer de suficientes medidas de seguridad.



La comprensión de estas situaciones pone de manifiesto la importancia de tener una buena gestión de contraseñas y unas buenas prácticas de seguridad para proteger nuestra información personal y confidencial.

ESTABLECER CONTRASEÑAS SEGURAS

Definir contraseñas seguras es crucial para proteger tus cuentas en Internet y tu información personal. Estas son algunas pautas clave para crear contraseñas seguras:

- **La longitud importa:** Intenta que tenga al menos entre 12 y 16 caracteres. Las contraseñas más largas son más seguras
- **Mezcla los caracteres:** Añade varios caracteres a tu contraseña incluyendo:
  - **Letras mayúsculas (A-Z)**
  - **Letras minúsculas (a-z)**
  - **Números (0-9)**
  - **Caracteres especiales (e.g., !, @, #, $)**

- **Evita patrones predecibles:** No uses una secuencia o repetitivos (como "12345" o "abcde"). Son muy fáciles de adivinar.
- **Sin información personal:** Evita utilizar tu nombre, fecha de nacimiento o palabras comunes. A menudo se pueden encontrar o adivinar en las redes sociales.
- **Palabras o frases poco comunes:** Utiliza una palabra o una frase aleatoria y poco común. Mejor aún, encadena varias palabras no relacionadas.
- **Piensa en una frase de contraseña:** Una secuencia de palabras o una frase es más fácil de recordar y puede ser larga, lo que la hace más segura. Por ejemplo, "TazaDeCafeEnLaMesa!".
- **Utiliza sustituciones no estándar:** Si utilizas palabras o frases, prueba a sustituir algunos caracteres, como usar "3" en lugar de "E" o "$" en lugar de "S".
- **Prueba tus contraseñas:** Hay muchas herramientas en línea que te permiten probar la solidez de tu contraseña (consejo: no utilices tu contraseña real). Puede darte alguna idea de lo fácil o difícil que es descifrarla.
- **Cambia las contraseñas con regularidad:** Aunque no siempre es necesario, sobre todo si utilizas una contraseña única y segura, cambiar las contraseñas con regularidad puede ser beneficioso, especialmente en el caso de las cuentas sensibles.
- **Mantente informado:** Conoce las mejores prácticas actuales para la seguridad de las contraseñas, ya que las recomendaciones pueden evolucionar con los cambios tecnológicos y las amenazas a la seguridad.

Si sigues estas indicaciones, podrás crear contraseñas seguras y eficaces que te ayudarán a proteger tu información digital. Recuerda que la fuerza de una contraseña no sólo reside en su complejidad, sino también en su carácter único e impredecible.

RECOMENDACIONES PARA LA GESTIÓN DE CONTRASEÑAS

La gestión eficaz de las contraseñas es crucial para mantener la seguridad y la privacidad en Internet. Aquí tienes algunas recomendaciones para gestionar las contraseñas:

- **Utiliza contraseñas fuertes y únicas:** Cada una de tus cuentas tiene que tener una contraseña única. Las contraseñas seguras suelen incluir una combinación de letras (mayúsculas y minúsculas), números y caracteres especiales. Evita palabras y frases comunes.

- **Utiliza un gestor de contraseñas:** Los gestores de contraseñas generan y almacenan contraseñas complejas por ti. Mantienen tus contraseñas seguras y accesibles a través de una contraseña maestra. Esto reduce la carga de recordar las contraseñas seguras.

- **Autenticación de 2 factores (2FA):** Siempre que sea posible, usa la autenticación de dos factores. Esto añade una capa adicional de seguridad al pedir una segunda forma de identificación además de la contraseña, como un código de mensaje de texto o una notificación de una aplicación.

- **Actualiza regularmente las contraseñas:** Cambia las contraseñas con regularidad, especialmente la del correo, el banco o las redes sociales. Sin embargo, no siempre es necesario si tienes contraseñas seguras y únicas.

- **Cuidado con los ataques de phishing:** **T**en cuidado con donde introduces tu contraseña. Los ataques de phishing suelen engañar a los usuarios para que introduzcan sus contraseñas en sitios web falsos. Comprueba siempre la URL del sitio web antes de introducir tus contraseñas.

- **Preguntas de seguridad:** Elige preguntas y respuestas de seguridad difíciles de adivinar. A veces, el nombre de tu madre o tu primer colegio pueden encontrarse en internet o adivinarse.

- **Supervisa tus cuentas en busca de fallos:** Usa servicios que te avisen si tu correo o contraseña se han visto comprometidos en una violación de datos. Esto te permitirá cambiar esa contraseña inmediatamente.

- **Evita usar información personal:** Ese tipo de información, como tu nombre, fecha de nacimiento o secuencias simples como "1234".

- **No compartas tus contraseñas:** Evita compartir tus contraseñas con otras personas. Si tienes que compartirla, cámbiala lo antes posible.

- **Haz copias de seguridad de con información de recuperación:** Asegúrate de que la información de recuperación de tu cuenta está actualizada. Esto incluye tu dirección de correo electrónico o número de teléfono para recuperar tus cuentas en caso de que olvides tu contraseña.

La clave para una gestión eficaz de las contraseñas es una combinación de contraseñas seguras y únicas, el uso de un gestor de contraseñas fiable y la vigilancia frente a las amenazas a la seguridad.

BACK 2 BASICS

5 MANUAL DE CIBERSEGURIDAD
CONCLUSIÓN

CONCLUSIÓN

A lo largo de este manual, hemos explorado la importancia de la crítica de la ciberseguridad y hemos profundizado en diferentes buenas prácticas y estrategias para protegerse contra las ciberamenazas más comunes. Al concluir este análisis, vamos a recapitular los puntos clave y a hacer hincapié en la importancia de aplicar estas prácticas en nuestra vida personal y profesional.

Lo primero y más importante, es mantener una buena higiene cibernética. Con la actualización periódica del software, el uso de contraseñas seguras y únicas, y la precaución al conectarse a redes Wi-Fi públicas, las personas pueden reducir significativamente el riesgo de ser víctimas de ciberataques. Las organizaciones también deben dar prioridad a la ciberhigiene mediante la aplicación de medidas de seguridad sólidas, la realización de auditorías de seguridad periódicas y la formación de sus empleados sobre prácticas seguras en línea.

En conclusión, lo más importante de este manual es que la ciberseguridad es una responsabilidad colectiva. Aplicando las buenas prácticas mencionadas en el manual, las personas y las organizaciones pueden reducir el riesgo de ser víctimas de ciberamenazas y proteger su información sensible, sus activos financieros y su reputación. La ciberseguridad no es un esfuerzo puntual, sino un compromiso permanente. Requiere educación, concienciación y adaptación continuas para ir un paso por delante de los ciberdelincuentes.

Recordemos que nuestro mundo digital evoluciona constantemente, al igual que las tácticas y técnicas empleadas por los ciberatacantes. Si nos mantenemos alerta, informados sobre

las nuevas amenazas y adaptamos nuestras defensas en consecuencia, podremos navegar por el panorama digital con seguridad y confianza.

Juntos, podemos construir un ecosistema digital más seguro y resistente en beneficio de todos.


universidade
de aveiro

BIO
LIVING

HELLENIC
REPUBLIC
UNIVERSITY
OF MACEDONIA

gri