Universidad Nacional de Tucumán
Facultad de Ciencias Económicas
Seguridad y Control en Sistemas Informáticos

PROPUESTA DE UN PLAN DE CAPACITACIÓN Y CONCIENTIZACIÓN EN CIBERSEGURIDAD EN EL MARCO DE LA FACULTAD DE CIENCIAS ECONÓMICAS - UNT

INTEGRANTES:

- **ÁLVAREZ, Sabouret Martín**
- **BERARDUCCI, Antonella**
- **FARÍAS, María Victoria**
- **URQUIZA, María Sol**
- **VALDEZ, Rodrigo Agustín**

Declaración jurada del origen de los contenidos:

Por medio de la presente, los autores manifiestan conocer y aceptar el “Reglamento para la Presentación de Trabajo Final” vigente de la asignatura “Seguridad y Control en Sistemas Informáticos”, haciéndose responsables por la totalidad de los contenidos del presente documento, los cuales son originales y de creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación nacional e internacional de Propiedad Intelectual.

Álvarez Sabouret, Martin. FIRMADO.

Berarducci, Antonella. FIRMADO.

Farías, María Victoria. FIRMADO.

Urquiza María Sol. FIRMADO.

Valdez, Rodrigo Agustín. FIRMADO.

Álvarez Sabouret Martín; Berarducci Antonella; Farías María Victoria; Urquiza María Sol; Valdez Rodrigo Agustín

Facultad de Ciencias Económicas UNT
martinras92@gmail.com ;anto.berarducci@gmail.com ;vicky.farias1995@gmail.com; Sol.medina389@gmail.com; rodrigo.valdez.cna.10@gmail.com

ÍNDICE

RESUMEN

El presente trabajo tiene como objeto de estudio la Facultad de Ciencias Económicas - Universidad Nacional de Tucumán. Ya que en el marco de tal institución educativa se detecta un desconocimiento parcial, y en otros casos total, por parte del personal docente, no docente y alumnos de la FACE hacia los temas relacionados a la seguridad de la información y sus riesgos, de modo que se encuentran potencialmente expuestos a una gran cantidad de posibles ataques informáticos peligrando no solo la información referida a la organización sino también a sus datos personales.

El objetivo principal del trabajo es elaborar un plan de concientización y capacitación para que todas las personas involucradas en la FACE tengan conocimiento (básicos y necesarios) sobre fraudes informáticos, engaños utilizando "Ingeniería Social", ciberataques, entre otros. Además, se busca que dichas partes conozcan sobre sus derechos, deberes y responsabilidades con respecto a la seguridad de la información, haciendo hincapié en las posibles consecuencias que podría generar un acto negligente que ponga en riesgo los activos de información de la organización, e incluso los personales.

Para ello, se recurrió a una extensa bibliografía para tener en cuenta un adecuado marco teórico en el presente trabajo.

Respecto a la metodología del trabajo, se recurrirá a un enfoque cualitativo, con un diseño "Investigación- Acción" basado en la recolección y análisis de datos de carácter cualitativo (tanto de fuentes primarias, a través de nuestras encuestas realizadas en el ámbito de la facultad, como de fuentes secundarias, a través del análisis de documentos vinculados), con el objetivo de comprender y resolver problemáticas específicas de la FACE vinculadas a la seguridad de información y detectar los problemas y vulnerabilidades presentes en el día a día, pudiendo así elaborar un plan de capacitación y concientización para resolver dicha problemática y cumplir con el objetivo previamente mencionado. Con el presente trabajo, se espera que el plan de capacitación propuesto, permita que la organización y sus integrantes obtengan conocimiento sobre Ciberseguridad y puedan estar al tanto de cómo protegerse ante un posible ataque informático. Y como medio de retroalimentación implementar a futuro, el cuestionario propuesto para evaluar el desempeño de dicho plan de capacitación y el nivel de madurez logrado. Como conclusión, consideramos que es fundamental que se desarrolle una cultura en seguridad informática en el ámbito académico, dado que, aunque las organizaciones inviertan mucho en dispositivos tecnológicos y en soluciones técnicas para proteger de manera adecuada los sistemas de información, si los usuarios no son conscientes de sus actos, toda la seguridad se ve comprometida.

PALABRAS CLAVE: Seguridad informática- Plan de capacitación– Vulnerabilidad Informática- Facultad de Ciencias Económicas UNT

INTRODUCCIÓN

Nuestro trabajo e investigación de campo se desarrolló en la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán. Una institución educativa orientada a la formación académica y profesional de sus alumnos.

Tras la cuarentena impuesta en gran parte del mundo debido al COVID-19, el proceso de digitalización de la sociedad avanzó a pasos agigantados. Gobiernos, universidades, empresas y personas, suman a la vida cotidiana nuevas herramientas y capacidades digitales de forma casi obligada. En este contexto, la tecnología ha pasado a tener un rol fundamental e indispensable para dar continuidad a la vida como la conocemos.

Frente a todo este cambio de cotidianidad, sumado a la falta de información y capacitación sobre la seguridad de información de la sociedad en general, aumentó exponencialmente el riesgo de ser víctima de un ciberataque. Los ciberdelincuentes han incrementado los ataques a las redes y sistemas informáticos de individuos, empresas, organizaciones globales o incluso hacia nuestra misma facultad, creando sitios Web, campañas de mails maliciosas con virus extorsivos, robando información, vulnerando aplicaciones como WhatsApp, y más. Lamentablemente esta es otra vulnerabilidad a la seguridad de la información que se agudizó en esta pandemia, por ello creemos que es necesario tener un conocimiento de qué es la seguridad de información, qué medidas deberían llevarse a cabo y cuáles son las amenazas a las que nos enfrentamos o podrían presentarse en el día a día en nuestra facultad, para así poder mitigar la mayor cantidad de riesgos posibles.

Un caso que podría tomarse como ejemplo, es el delito informático que tuvo como víctima a la UADE (Universidad Argentina de la Empresa) de la provincia de Buenos Aires. En este caso, un alumno fue capaz de vulnerar el sistema de dicha institución a través de un malware en la página de la UADE, logrando así, no solo acceder a la base de datos de alumnos, profesores y usuarios de la red, sino también modificar las notas de exámenes y trabajos.

DESARROLLO DEL PROBLEMA

Desconocimiento parcial, y en otros casos total, por parte del personal docente, no docente y alumnos de la FACE hacia los temas relacionados a la seguridad de la información y sus riesgos, de modo que se encuentran potencialmente expuestos a una gran cantidad de posibles

ataques informáticos peligrando no solo la información referida a la organización sino también a sus datos personales.

PREGUNTAS DE INVESTIGACIÓN

1. ¿Cómo se puede capacitar y concientizar tanto al personal como a los miembros implicados en la organización?
2. ¿El responsable de TI designado por la FACE conduce a la organización para el cumplimiento de los temas relacionados con la Seguridad/Ciberseguridad de la misma?
3. ¿Las personas que forman parte de la FACE (alumnos, docentes y no docentes) están al tanto de cómo protegerse de un ciberataque?

OBJETIVO GENERAL

Elaborar un plan de concientización y capacitación para que todas las personas involucradas en la FACE tengan conocimiento sobre fraudes informáticos y engaños utilizando "Ingeniería Social", entre los que se destacan estar al tanto sobre sus derechos, deberes y responsabilidades con respecto a la seguridad de la información, haciendo hincapié en las posibles consecuencias ante un acto negligente que ponga en riesgo los activos de información de la organización y personales.

OBJETIVO ESPECÍFICOS

- Elaborar un modelo de entrevista semi estructurada dirigida al responsable de TI de la Facultad de Ciencias Económicas- UNT, con el objetivo de conocer si cumplen con los requisitos de seguridad deseados y utilizar como input para elaborar a futuro un análisis de madurez seguridad de la información.
- Proponer un modelo de cuestionario destinados a alumnos, docentes y no docentes de la Facultad de Ciencias Económicas-UNT para implementar con posterioridad al plan de capacitación y de esa manera evaluar el desempeño de dicho plan.

METODOLOGÍA

En cuanto a la metodología el trabajo tendrá un enfoque cualitativo, ya que se recolectarán y analizarán información sobre el grado de conocimiento, opiniones, comportamientos y experiencias de alumnos,

docentes y no docentes sobre la ciberseguridad en la facultad de ciencias económicas.

Dentro del enfoque cualitativo, el diseño más apropiado para el presente trabajo es el diseño "Investigación- Acción" ya que lo que se busca con el trabajo es comprender y resolver problemáticas específicas de una colectividad vinculadas a un ambiente, en este caso la Facultad de Ciencias Económicas. Primero se busca detectar el problema de investigación y luego formular un plan o programa para resolver la problemática. En este caso un plan de concientización, lo que incluye implementar el plan, evaluar resultados y por último la retroalimentación, la cual conduce a un diagnóstico y a una nueva espiral de reflexión y acción. A su vez, el diseño es participativo ya que intervienen de manera aún más colaborativa y democrática uno o varios investigadores y participantes o miembros de la comunidad involucrada.

Para las herramientas de recolección se utilizará como fuente primaria, la observación directa en el ámbito educativo de la facultad de ciencias económicas, para indagar sobre el comportamiento de docentes, no docentes y alumnos con respecto aspectos de la seguridad de la información, también se utilizará como fuentes de datos secundarios (documental) se recolectará y analizará, documentos, bibliografía sobre seguridad de la información, así como lo referente a cómo elaborar un plan de capacitación y concientización.

Con respecto a la muestra, será un muestreo no probabilístico por conveniencia. Ya que se observará a alumnos, docentes y no docentes que forman parte de la facultad de Ciencias Económicas de la Universidad Nacional de Tucumán.

MARCO TEÓRICO

Seguridad de la información:

La seguridad informática o de la información es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. **(Urbina Baca Gabriel,2016, p.12)**

Plan de concientización:

"Un plan de concientización tiene el objetivo de educar a los colaboradores de tu empresa en seguridad de la información. De esta manera, el personal estará capacitado y preparado para mantener el programa de seguridad". En otras palabras, este plan te permitirá seguir una

ruta de cursos, certificaciones, capacitaciones y/o campañas de e-mail para cumplir con los objetivos de tu negocio y acompañar tu estrategia de seguridad. ***Araujo, A. (septiembre 16,2021).*****ISO 27001: ¿Cómo crear el plan de concientización y capacitación de tu empresa? https://blog.hackmetrix.com/plan-de-concientizacion-y-capacitacion-seguridad/.**

Vulnerabilidades Informática:

Una vulnerabilidad (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos. **INCIBE.(Marzo 20,2017).Amenaza vs Vulnerabilidad, ¿Sabes e que se diferencian?https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-deferencian**

Fuente: Instituto Nacional de Ciberseguridad (INCIBE)

Amenazas Informática:

Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas. **INCIBE. (Marzo 20,2017). Amenaza vs Vulnerabilidad, ¿Sabes e que se diferencian? https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-deferencian**

Análisis de riesgo:

Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo. **INCIBE. (Octubre 10,2020). Glosario de términos de ciberseguridad, aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf**

Virus Informático:

Un virus informático es un software diseñado para causar daños de diferente tipo en una computadora o una red de computadoras, alterando el código del software original que tenía la computadora y haciendo que ésta trabaje de manera anormal. Algunos virus pueden causar tanto daño como incapacitar a un disco duro, haciendo que se pierda toda la información, o bloquear el funcionamiento de una red; los menos dañinos sólo provocan molestias en el funcionamiento de la computadora. **(Urbina, Baca Gabriel,2016, p.173)**

Phishing:

Es una forma de ataque informático donde, mediante el uso de correo electrónico o sitios web maliciosos, los atacantes solicitan información personal haciéndose pasar por una organización legal o altruista.(**Urbina, Baca Gabriel,2016,p.200)**

Antecedentes:

Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información" Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones UNIVERSIDAD PEDAGÓGICA Y TECNOLÓGICA DE COLOMBIA

DESARROLLO

Propuesta del Modelo de Entrevista Semi Estructurada dirigido a responsable de TI de la Facultad de Ciencias Económicas, para conocer el grado de madurez en seguridad de la información

1. La facultad de ciencias económicas ¿ha designado un responsable que pueda conducir a la organización para el cumplimiento de los temas relacionados con la Seguridad/Ciberseguridad de su organización?
2. ¿Cómo está organizada el área de seguridad de la información, siendo un factor determinante para lograr la mejor gestión de la seguridad?
3. ¿La FACE, tiene definida una Política de Seguridad de la Información?
4. ¿Cumple o debe cumplir con alguna normativa legal o marco regulatorio?
5. Los riesgos inherentes a la información en caso de materializarse podrían ocasionar daños o pérdidas económicas, de imagen, legales u otros a la organización ¿Existe un proceso para la gestión de los riesgos?
6. ¿La FACE definió un proceso periódico que permite generar y mantener actualizados los inventarios de elementos tecnológicos de la organización Servidores, estaciones de trabajo, equipos de comunicación, impresoras, ¿entre otros?
7. ¿Los usuarios que administran sistemas deben utilizar una cuenta personal exclusiva para la administración y otra cuenta distinta de privilegios acotados para uso personal (correo, ofimática, etc.) ¿Se cumple?
8. ¿Se realizan regularmente copias de respaldo de todos los datos de sistemas de manera automatizadas?
9. ¿Implementó la institución un plan de seguridad y respuesta a incidentes de Seguridad?
10. ¿Implementó la facultad un proceso de educación y awareness en seguridad de la información a sus empleados?
11. ¿Se asegura que todos los usuarios están informados y capacitados para cumplir con sus deberes y responsabilidades relacionados a seguridad cibernética?
12. ¿Se han establecido métricas e indicadores para medir la eficacia de las acciones desarrolladas como parte del Programa de Concientización?

Propuesta del Modelo de Cuestionario dirigido a alumnos, docentes y no docentes de la Facultad de Ciencias Económicas

1. ¿Cuán importante es para vos la ciberseguridad?
   Nada importante……. Poco importante……. Importante…. Muy importante……
2. ¿Sabes lo que es la autenticación de doble factor?
   Sí……. No…….
3. ¿Has implementado medidas de ciberseguridad en tus redes sociales y dispositivos?
   Sí……. No…….
4. ¿Cuáles?
   Doble Factor……. Contraseña……
   Patrón…… Datos biométricos (Huella, rostro, etc.) …….
   Antivirus…... Firewall…….
   Otros: .....
5. ¿Tienes diferentes claves configuradas para tus distintas cuentas?
   Sí…… No……
6. ¿Sabes que es el phishing?
   Sí…… No…….
7. ¿Sabes lo que es el ransomware?
8. Sí……. No…….
9. ¿Sabes qué medidas puedes tomar para evitar el robo de tus cuentas de redes sociales como WhatsApp?
   Sí……. No…….
10. ¿Cuáles?……
11. ¿Sabes lo que es una contraseña robusta?
    Sí……. No…….
12. ¿Sabes lo que es un back up o una copia de respaldo?
    Sí……. No…….
13. ¿Sabías que en caso de que te roben alguna cuenta, se ponen en riesgo todos tus contactos?
14. Sí……. No…….
15. ¿Alguna vez fuiste víctima de alguna estafa virtual? Ya sea si te robaron las cuentas o alguien se hizo pasar por un amigo tuyo.
    Sí……. No…….
16. ¿Alguna vez recibiste algún tipo de capacitación para evitar estafas por internet?
    Sí……. No…….

Propuesta de Plan de Capacitación y Concientización

OBJETIVO DEL PLAN

Establecer pautas para que los miembros de la FACE-UNT, asuman la responsabilidad personal de proteger la información de la organización.

DESCRIPCIÓN.

El contenido del programa será determinado en base a las tendencias globales relacionadas con las potenciales vulnerabilidades inherentes a las operatorias que lleva adelante la FACE y a las actividades de la vida diaria en general de los miembros de la misma.

ALCANCE.

Durante las actividades serán abordados diversos aspectos relacionados con las problemáticas inherentes a los riesgos y amenazas que afectan la confidencialidad, integridad y disponibilidad de la información.

ABORDAJE.

Se detallan a continuación los aspectos relevantes que serán incorporados durante su abordaje:

- Ingeniería Social
- Seguridad del Correo Electrónico
- *Phishing*
- *Smishing*
- *Vishing*
- *Malware* (Virus – *Ransomware*)
- Seguridad en Redes Sociales (Privacidad)

DISTRIBUCIÓN DE LA INFORMACIÓN

En función de lo expuesto precedentemente, la Dirección de Informática utilizará diversos formatos para la entrega periódica de conocimiento, tanto a personal interno como a los alumnos de la facultad.

- Cadenas de correo electrónico con recomendaciones y cuestionarios.
- Recomendaciones de seguridad a través de *flyers* en el campus virtual.

- Recomendaciones de seguridad utilizando las carteleras de los espacios públicos.

RECURSOS.

El plan será actualizado por el Departamento de Informática de la FACE y lo ejecutará el personal correspondiente, mediante difusiones masivas de correos electrónicos, actualización del Campus Virtual y de las distintas cuentas de Instagram mencionadas en el cronograma.

CRONOGRAMA

Comunicaciones Antifraude		
Tema	Fecha	Título
Campus Virtual	06/02/2023 al 14/02	¿Qué es el Phishing?
	15/02/2023 al 28/02/2023	¿Qué es el Smishing?
	01/03/2023 al 15/03/2023	¿Qué es el Vishing?
	16/03/2023 al 31/03/2023	Tips antifraudes. Alerta por estafas telefónicas
	01/04/2023 al 15/04/2023	Tips de seguridad. Alerta por estafas por WhatsApp
	16/04/2023 al 30/04/2023	¿Qué hacer ante un ataque de ransomware?

	01/05/2023 al 15/05/2023	Tips Anti Fraude HOT SALE
	16/05/2023 al 31/05/2023	Autenticación doble factor
	01/06/2023 al 15/06/2023	¿Es necesario publicar el minuto a minuto de nuestra vida?
Mails	16/11/2022	Tips Mundiales
	09/01/2023	¿Qué es el Phishing?
	08/04/2023	¿Qué es el Smishing?
	16/04/2023	¿Qué es el Vishing?
	05/06/2023	Tips antifraudes. Alerta por estafas telefónicas
	08/07/2023	Tips de seguridad. Alerta por estafas por WhatsApp
	23/07/2023	¿Qué hacer ante un ataque de ransomware?
	27/07/2023	Tips Anti Fraude HOT SALE
	16/11/2022	Tips Mundiales

Instagram de la FACE del Instituto de Administración, del Centro de Estudiantes, de Bienestar Estudiantil	16/06/2023	Autenticación doble factor
	30/03/2023	¿Es necesario publicar el minuto a minuto de nuestra vida?

RECOMENDACIONES

Luego de implementar el plan de capacitación se recomienda elaborar el cuestionario propuesto en el trabajo para determinar la efectividad en la implementación del mismo sirviendo como retroalimentación para la mejora continua de las acciones a implementar en materia de seguridad informática. Otro apartado es llevar a cabo la entrevista propuesta hacia el o los responsables del área de TI (tecnología de la información) a fin de tener noción de la madurez en la gestión de la seguridad. Como también la distribución del cuestionario hacia alumnos, docentes y no docentes de la Facultad de Ciencias Económicas con lo que se determinará el nivel de conocimiento y cultura al respecto de la ciberseguridad.

Como recomendaciones de seguridad se plantean a continuación las buenas prácticas recomendadas por expertos en la materia, se procedió a indagar en diferentes fuentes para tener un gran abanico de herramientas para implementar en la institución académica.

Las siguientes son recomendaciones sugeridas por el Instituto Nacional de Ciberseguridad Español en su artículo (INCIBE, Desarrollar Cultura en Seguridad, 2020) las cuales consideramos pertinentes de aplicar en la facultad de ciencias económicas.

Como recomendaciones se sugiere:

Fuente: (INCIBE, 2020)

El personal técnico del Departamento de Informática es quien precisa más formación en materia de seguridad y con un mayor grado de especialización. Se debe poner a disposición de los administradores de sistemas los recursos y mecanismos adecuados para formarse o autoformarse en aspectos relacionados con la seguridad de los sistemas y aplicaciones que dan soporte a los procesos de negocio de nuestra organización. Dentro de estos aspectos podemos señalar algunos tan críticos como:

Fuente: (INCIBE, 2020)

La seguridad hoy en día no se debe limitar sólo a los aspectos técnicos, sino que debe incorporar otros ámbitos como el organizativo y el legal.

Dado la sensibilidad de información con la que cuenta la Facultad de Ciencias Económicas de la UNT, resulta fundamental la formación en el ámbito de protección de datos de carácter personal, puesto que el nivel de riesgo asociado puede ser muy alto. El tratamiento de los datos como ser de todo el alumnado debe realizarse partiendo de unas determinadas condiciones, tanto a nivel técnico como legal.

En definitiva, todo el personal de la organización con acceso a los sistemas de información corporativos debe recibir formación relacionada con buenas prácticas en materia de seguridad en su puesto de trabajo y en el desempeño de sus funciones.

Cabe resaltar algunas de las recomendaciones que debería tener el personal para protegerse ante eventuales ataques:

Fuente: (INCIBE, 2020)

La formación y la normalización de los protocolos de trabajo en la Face-UNT formarían parte de los controles preventivos orientados a mejorar el nivel de seguridad de la organización.

Una vez definido el marco de trabajo y trasladado a las partes afectadas, será necesario comprobar que efectivamente se está siguiendo y aplicando. Para ello, deberá existir un responsable de Seguridad encargado de velar por:

► La vigencia y correspondiente actualización de las normas y procedimientos definidos, atendiendo a la detección de nuevas situaciones, de cambios legislativos y organizativos, de prácticas tecnológicas en la organización que recomienden la revisión de los mismos.

► La implantación de los mismos y su cumplimiento por parte de los empleados.

A continuación, se citan algunos temas sobre los que hay que concientizar a los empleados:

► Uso seguro de redes wifi.

► Uso seguro del correo electrónico.

► Prácticas de navegación segura.

► Identificación de virus y malware.

► Gestión de contraseñas.

► Clasificación de la información.

► Borrado seguro de la información.

► Uso de dispositivos USB.

► Seguridad en dispositivos móviles.

► Uso de programas de mensajería instantánea.

► Riesgos de las redes sociales.

► Técnicas de ingeniería social.

► Mesas limpias.

► Destrucción segura de la documentación en soporte papel.

► Posibles escenarios de fuga de información.

En cuanto a las prácticas del empleado seguro en su lugar de trabajo (Technology, 2021) nos da la noción de las mismas argumentando que además de las políticas de seguridad que los miembros de la organización

deben cumplir, existen otras prácticas que contribuyen a aumentar la seguridad.

Entre ellas se incluyen:

- El empleado tiene la responsabilidad de utilizar adecuadamente todos los activos de la organización, como también de proteger aquellos que estén bajo su resguardo.
- Se deben bloquear los equipos cuando se los desatiende, incluso cuando se deja por pocos minutos el puesto de trabajo, para evitar la extracción o lectura de información por parte de terceros no autorizados.
- Se debe mantener el escritorio limpio, tanto en la vida física como en los sistemas operativos, para no divulgar información sensible accidentalmente.
- Cuando se sospecha que un sistema, o incluso la red completa de la institución, ha sido comprometida, se debe dar aviso al departamento de seguridad o de TI de manera inmediata.
- Más aún, cuando un incidente efectivamente sucede es indispensable avisar rápidamente al departamento pertinente.

Para tener otras referencias sobre el tema y otorgar un mayor espectro de recomendaciones, en (Scolnik, 2016) tenemos puntualmente prevenciones a los siguientes tipos de ataques:

INTRUSIONES: Los hackers intentan penetrar los dispositivos de muchas maneras distintas. Incluso pueden usar la cámara de video para espiar. La solución es tener instalado un cortafuego (denominado “firewall” en inglés).

ENCRIPTACIÓN DE DATOS: Para proteger la información sensible lo mejor es encriptar los datos y afortunadamente hay software recomendable y gratuito, tanto para proteger archivos como discos (por ej.: www.truecrypt. org).

ACCESO A SITIOS WEB: Los sitios seguros se identifican por un candadito de color amarillo. Hay que clickear en ellos para comprobar que no sean sólo una imagen y verificar el certificado digital que protege las transacciones con esos sitios.

USO DE MAIL: Los mails presentan diversos problemas de seguridad y la mejor manera de protegerlos es usando certificados digitales que permiten, si el destinatario también posee uno, encriptar el contenido. Otra posibilidad es escribir un documento, encriptarlo con una clave secreta, y

mandarlo como adjunto de un mail normal. Como otra medida de seguridad los “webmails” más populares ocultan la dirección IP del remitente con el objeto de evitar su identificación.

MANEJO DE CONTRASEÑAS: La gran mayoría de los problemas de seguridad se generan por el uso de contraseñas inseguras. Esto es lógico pues para operar con mails, bancos, etc., debemos memorizar una gran cantidad de ellas. Es por eso que recurrimos a emplear claves basadas usualmente en nombres propios, cumpleaños u otros datos memorizables. De hecho, no se nos ocurre usar algo más seguro como ser: “hY&%0!!”€€@#Uzj398\ñ/”.

La mejor solución es recurrir a un programa para administrar claves . En la Web se pueden encontrar varios disponibles, eficientes y sin cargo. El mismo exige memorizar una sola clave maestra, e internamente se pueden almacenar todas las claves que se necesiten, incluso el programa mismo las puede llegar a generar. No importa que sean difíciles de recordar dado que con un click se las copia al portapapeles para emplearlas donde se necesiten. Es importante destacar que hay de dos tipos: los que se comunican con la web y los que no. Los primeros deben evitarse en temas que requieran máxima seguridad. Algunos ofrecen el “auto-rellenado de formularios” y para ello almacenan en la web nuestros datos básicos, lo cual puede considerarse como algo no recomendable.

FLYERS PUBLICITARIOS para la campaña de concientización en seguridad informática

Otra de las propuestas es la difusión de información a todos los implicados en la institución educativa a modo de Flyers para la capacitación y concientización sobre la seguridad informática. A modo de ejemplo se elaboraron los siguientes modelos de promoción de ciberseguridad:


¡EVITEMOS EL PHISHING!
Una forma de verificar si fuiste víctima de una ataque de phishing es revisar en forma periódica tus resúmenes bancarios buscando transferencias que no autorizaste.
¡PRESTÁ MUCHA ATENCION A TUS CORREOS!
¿QUÉ ES EL PHISHING?
Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas.
¿QÚE MEDIOS UTILIZAN?
El método más utilizado es el correo electrónico falso.
Estos correos electrónicos pueden aparecer como comunicaciones de bancos, servicios de pago, mercados de compra en línea o proveedores de servicios públicos.
¿QUÉ DATOS DESEAN OBTENER?
• Nombres de usuario y contraseñas
• Datos bancarios
• Datos de tarjetas de crédito-
Con estos datos los ciberdelincuentes pretenden hacerse pasar por nosotros y realizar compras y transacciones web
¿CÓMO NOS PROTEGEMOS?
• Chequear el remitente. Suelen ser parecidos a los oficiales
• Chequear la redacción y la ortografía.
• No responder mensajes que solicitan información personal o privada.
• No hacer clic. En algunos casos el correo es una imagen, no hagas clic en ningún sitio del cuerpo del correo ni siquiera en la barra lateral..
• No brindar contraseñas. Ninguna comunicación oficial solicita datos como contraseña o DNI a través del correo electrónico.
A LA SEGURIDAD LA HACEMOS ENTRE TODOS
FACULTAD DE CIENCIAS ECONOMICAS
UNIVERSIDAD NACIONAL DE TUCUMAN

TIPS DE SEGURIDAD MUNDIALES

SE ACERCA EL MUNDIAL DE LA FIFA

Los eventos deportivos mundiales son un gran atractivo en cuanto a pasión e interés que generan en las personas.
Los ciberdelincuentes aprovechan este interés y la falta de cuidado y atención de los fanáticos del deporte para engañarnos y cometer sus delitos.

¿CÓMO NOS ENGAÑAN?

Prometen cosas que parecen reales y son muy tentadoras. Sin embargo, son falsas y sólo tienen una intención: Robar nuestros datos privados. Los mismos pueden ser contraseñas , datos de tarjetas de crédito o de cuentas bancarias.

¿QUÉ PROMETEN?

- Entradas para asistir al evento
- Reservas de vuelos y alojamientos
- Descuentos y sorteos de todo tipo, relacionados con entradas, viajes y alojamientos
- Transmisión del evento en vivo mediante Internet
- Noticias de último momento de gran relevancia

¿QUÉ MEDIOS UTILIZAN?

Los medios más utilizados por los ciberdelincuentes son el correo electrónico, publicaciones y mensajes en redes sociales, publicidades en sitios web y hasta mensajes de texto.

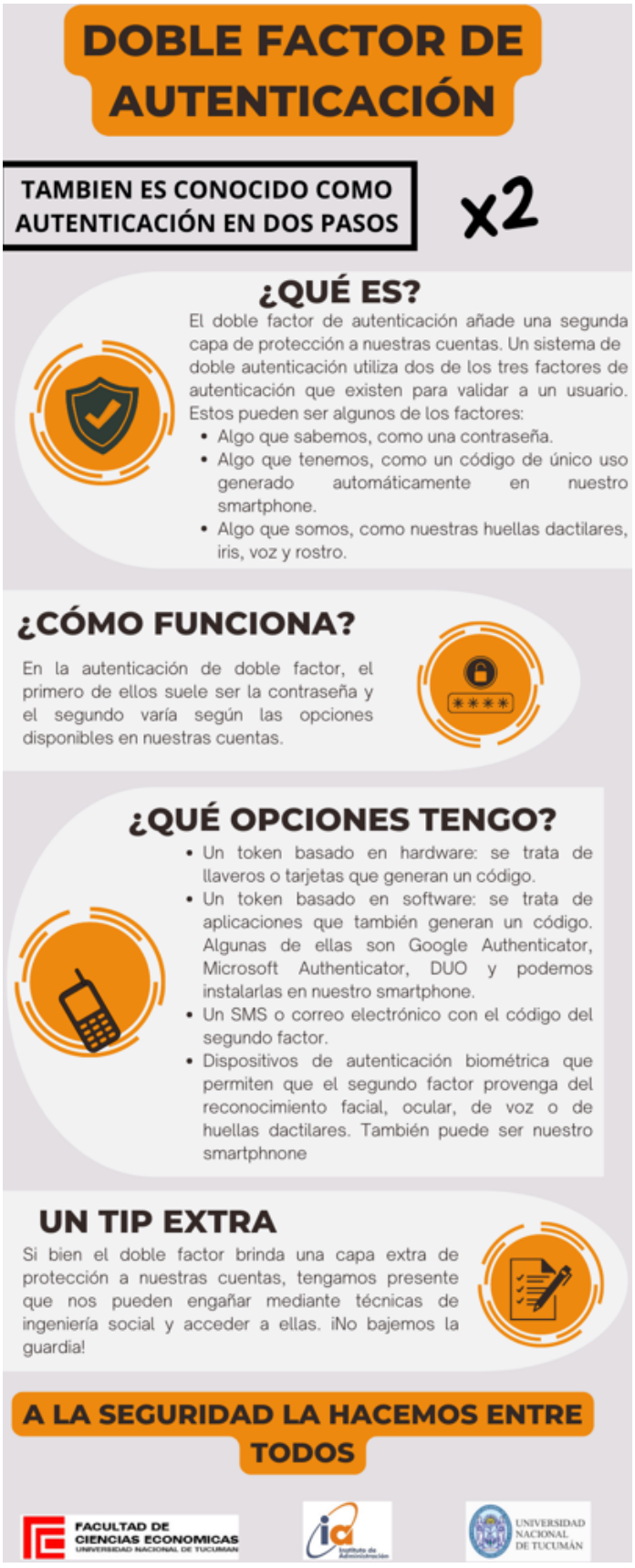
¿CÓMO NOS PROTEGEMOS?

Para todo lo referido a compras, descuentos o sorteos, debemos ingresar por nuestra cuenta al sitio oficial que lo ofrece, sin seguir ningún enlace.
Para noticias, debemos ingresar a nuestro sitio de noticias de confianza directamente y buscar allí la noticia que deseamos ver.
Para ver el evento en Internet, debemos hacerlo a través de un sitio oficial de deporte que ofrezca dicha posibilidad. Las alternativas no oficiales y gratuitas suelen ser las más peligrosas.

A LA SEGURIDAD LA HACEMOS ENTRE TODOS

FACULTAD DE CIENCIAS ECONOMICAS
UNIVERSIDAD NACIONAL DE TUCUMAN

UNIVERSIDAD NACIONAL DE TUCUMÁN


DOBLE FACTOR DE AUTENTICACIÓN
TAMBIEN ES CONOCIDO COMO AUTENTICACIÓN EN DOS PASOS
x2
¿QUÉ ES?
El doble factor de autenticación añade una segunda capa de protección a nuestras cuentas. Un sistema de doble autenticación utiliza dos de los tres factores de autenticación que existen para validar a un usuario. Estos pueden ser algunos de los factores:
• Algo que sabemos, como una contraseña.
• Algo que tenemos, como un código de único uso generado automáticamente en nuestro smartphone.
• Algo que somos, como nuestras huellas dactilares, iris, voz y rostro.
¿CÓMO FUNCIONA?
En la autenticación de doble factor, el primero de ellos suele ser la contraseña y el segundo varía según las opciones disponibles en nuestras cuentas.
¿QUÉ OPCIONES TENGO?
• Un token basado en hardware: se trata de llaveros o tarjetas que generan un código.
• Un token basado en software: se trata de aplicaciones que también generan un código. Algunas de ellas son Google Authenticator, Microsoft Authenticator, DUO y podemos instalarlas en nuestro smartphone.
• Un SMS o correo electrónico con el código del segundo factor.
• Dispositivos de autenticación biométrica que permiten que el segundo factor provenga del reconocimiento facial, ocular, de voz o de huellas dactilares. También puede ser nuestro smartphnone
UN TIP EXTRA
Si bien el doble factor brinda una capa extra de protección a nuestras cuentas, tengamos presente que nos pueden engañar mediante técnicas de ingeniería social y acceder a ellas. ¡No bajemos la guardia!
A LA SEGURIDAD LA HACEMOS ENTRE TODOS
FACULTAD DE CIENCIAS ECONOMICAS
UNIVERSIDAD NACIONAL DE TUCUMÁN


¿QUÉ HACER ANTE UN ATAQUE RANSOMWARE?
¡NO ENTRAR EN PÁNICO!
¿QUÉ ES UN RANSOMWARE?
Es un software malicioso que encripta los archivos y hasta sistemas operativos enteros, para luego pedir un rescate a cambio de devolver el acceso a los mismos.
¿QÚE MEDIOS UTILIZAN?
Los medios más utilizados son:
• El pshishing.
• Publicidades falsas
• Cadenas falsas de whastapp
• Sitios web infectados
¿QUÉ HACER?
No entrar en pánico. A menudo los ciberdelincuentes utilizan técnicas como colocar mensajes de alerta, enlistar los archivos encriptados y colocar un temporizador, para hacer que actuemos rápido.
Se aconseja no pagar, porque no tendremos la certeza de recuperar nuestra información. estamos tratando con un delincuente. En caso de brindarles dinero, estaremos financiando una actividad delictiva.
¿CÓMO NOS PROTEGEMOS?
• Mantener el software actualizado
• Mantener copias de seguridad (se recomiendan al menos dos en caso de que alguna falle)
• Utilizar bloqueador de publicidad
• Utiizar antivirus
• Mantener el antivirus actualizado
A LA SEGURIDAD LA HACEMOS ENTRE TODOS
FACULTAD DE CIENCIAS ECONOMICAS
UNIVERSIDAD NACIONAL DE TUCUMÁN

CONCLUSIONES

Consideramos que es fundamental que se desarrolle una cultura en seguridad informática en el ámbito académico, dado que por más que se cuente con el mejor sistema de gestión en seguridad, tal como menciona (INCIBE, Desarrollar Cultura en Seguridad, 2020), ***"Una cadena es tan fuerte como su eslabón más débil"***, siendo el eslabón más débil las personas, usuarios de los sistemas.

Es decir, aunque las organizaciones inviertan mucho en dispositivos tecnológicos y en soluciones técnicas para proteger de manera adecuada los sistemas de información, si los usuarios no son conscientes de sus actos, toda la seguridad se ve comprometida.

Para cambiar esta situación, es necesario invertir también en la formación en seguridad a los usuarios. Siendo conscientes de que:

- La mayor amenaza para una organización y sus datos no proviene del exterior, se origina en sus propios empleados. Ya sea por ignorancia, o de forma intencionada, tienen el potencial de poner sus datos en riesgo.
- Los errores que nacen de la ignorancia y el descuido no son lo único de lo que preocuparse, los empleados insatisfechos, frustrados y codiciosos pueden ser una amenaza igual de grande, quizás incluso mayor. En particular, si trabajan en TI, un empleado sabe cómo funcionan sus sistemas y dónde se encuentran las vulnerabilidades.
- Es fundamental tomar medidas que protejan contra personas internas maliciosas y mitiguen la amenaza que representa el error de los empleados.

POR LO QUE SERÁ PRIMORDIAL:

Fomentar una cultura de educación, conciencia y ciberseguridad, lo que implicará entender la seguridad corporativa, aplicar controles tecnológicos y de gestión, seguir las buenas prácticas, mantener a los usuarios educados y conscientes en temas de seguridad de la Información, generando consecuentemente un valor agregado a la organización. Todos estos elementos en conjunto contribuyen a mantener la confidencialidad, integridad y disponibilidad de la información, además de perseguir un propósito de mayor alcance e importancia: proteger a todos los implicados.

BIBLIOGRAFÍA

Amezquita Becerra, G. (2022). *Plan de capacitación, sensibilización y comunicación de la seguridad de la información.* Colombia: UPTC.

Araujo, A. (16 de Septiembre de 2021). *ISO 27001: ¿Cómo crear el plan de concientización y capacitación de tu empresa?* Obtenido de hackmetrix: https://blog.hackmetrix.com/plan-de-concientizacion-y-capacitacion-seguridad/

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* México: Grupo Patria.

CISCO. (18 de mayo de 2017). *Cisco Networking Academy*. Obtenido de https://campus2.unt.edu.ar/pluginfile.php/149897/mod_resource/content/2/Crear%20y%20almacenar%20contrase%C3%B1as%20seguras.pdf

Escrivá Gascó, G., Romero Serrano, R., Ramada, J. D., &Onrubia Pérez, R. (2013). *Seguridad Informática.* España: Macmillan Profesional.

INCIBE. (20 de Marzo de 2017). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* Obtenido de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INCIBE. (5 de Febrero de 2020). *Concienciación y Formación-Políticas de seguridad*. Obtenido de https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/concienciacion-y-formacion.pdf

INCIBE. (2020). *Desarrollar Cultura en Seguridad.* España: Ministerio de Asuntos Económicos y Transformación Digital.

INCIBE. (10 de Octubre de 2020). *Glosario de términos de ciberseguridad, aproximación para el empresario*. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Laudon, J. P., & Laudon, K. C. (2016). *Administración de los Sistemas de Información, Organización y Tecnología.* México: Prentice Hall Hispanoamericana.

Scolnik, H. (2016). *Seguridad.* Buenos Aires, Argentina: CNEA.

Technology, E. E. (26 de Noviembre de 2021). *Guía del Empleado Seguro*. Obtenido de https://empresas.eset-la.com/archivos/novedades/52/guia-empleado-seguro-eset.pdf