UNIDAD DE CONOCIMIENTO

Octubre 2020

Ciberseguridad y Recursos Humanos

"Si crees que la tecnología puede solucionar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología."

Bruce Schneier

fundació factor humà

¿Qué es?

Toda organización tiene la obligación de proteger la información confidencial a la que tiene acceso gracias al ejercicio diario de su actividad. Por eso, especialmente en un momento en el cual el teletrabajo se ha convertido en algo masivo y las acciones ofensivas contra sistemas de información se han incrementado significativamente, las empresas deben poner el foco en la ciberseguridad y destinarle recursos.

- ✓ La **ciberseguridad**, también conocida como **seguridad de la información electrónica** o **seguridad de tecnología de la información**, "es la práctica de defender los ordenadores, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos", tal y como lo define la compañía internacional dedicada a la seguridad informática Kaspersky. Este concepto es aplicable tanto en el ámbito doméstico como en el de los negocios y, en este último caso, implica especialmente a dos departamentos: el de Tecnología de la Información y el de Recursos Humanos.

  - Aunque tradicionalmente se ha relacionado esta materia con el Área de Tecnología de la Información, la **función de Personas** de una organización también debe tener incidencia en el ámbito de la ciberseguridad, teniendo en cuenta que una incorrecta forma de proceder por parte de los miembros de la plantilla puede generar una situación de vulnerabilidad para el sistema de información. Al mismo tiempo, es importante tener presente que una de las mejores medidas de prevención de ciberamenazas que puede tener cualquier empresa es la formación y concienciación de las propias personas trabajadoras. Además, el papel que juega también puede ser clave en caso de que no se haya podido evitar que la empresa sea víctima de un ciberataque, siendo fundamental en su gestión.

  - **¿Qué puede hacer el Departamento de Recursos Humanos para implicarse en la prevención y gestión de ciberataques?** Tal y como se explica en el blog "Más que nómina" de la compañía Seresco, el Área de Personas puede **organizar jornadas de concienciación** entre los/as empleados/as para que entiendan mejor cuáles son los riesgos y, además, puede **facilitar una formación en seguridad** adecuada a su nivel. Por otra parte, es importante que participe en la **revisión de los procedimientos de seguridad** con el objetivo de mejorar su adaptación a los diferentes puestos de trabajo y que **revise los procedimientos de alta y baja de las personas trabajadoras** para asegurar que se estén haciendo correctamente.

Finalmente, este Departamento también puede tener un papel esencial a la hora de realizar simulacros de ataques por ingeniería social, que permiten evaluar el grado de concienciación de los/as trabajadores/as respecto a este tipo de amenazas.

- Prácticas como esta última son cada vez más habituales en las empresas. Por eso, la figura del ***hacker* ético** ha cogido relevancia en los últimos tiempos. Tal y como se expone en el blog de Iberdrola, los *hackers* éticos tienen como objetivo reforzar la seguridad informática de las organizaciones llevando a cabo ataques que permitan evaluarla. Generalmente son parte de la plantilla de grandes empresas, pero también puede tratarse de profesionales externos que actúan como consultores a través de empresas de ciberseguridad. Gracias al *hacking* ético las organizaciones pueden detectar vulnerabilidades y están mucho más preparadas en caso de que la ciberamenaza sea real.

- En definitiva, es evidente que la ciberseguridad es una cuestión trascendente para las organizaciones. Sin embargo, el incremento de medidas aplicadas por las empresas puede hacer aflorar un nuevo debate: ¿es posible que se utilice el argumento de la seguridad para someter a los trabajadores a un mayor control? Es fundamental que las organizaciones encuentren el equilibrio entre la privacidad de las personas y la seguridad de la empresa.

Herramientas

Para evitar que el sistema de información de una empresa sufra ciberataques, o al menos reducir el riesgo, es importante que tanto los/as empleados/as como la propia organización adopten las medidas de protección y prevención adecuadas. Según se expone en el artículo de la revista Capital Humano basado en una guía elaborada por EY *Diez Medidas para protegerse de los ciberataques en tiempos de la Covid-19*, algunas de las medidas más recomendables son:

- **Utilizar siempre que sea posible los ordenadores de la empresa**, ya que disponen de las medidas de seguridad óptimas. En caso de que no sea posible y se tenga que optar por utilizar ordenadores personales, se recomienda que el Departamento de Tecnología de la Información les dé previamente el visto bueno.

- **Gestionar y utilizar adecuadamente el correo electrónico**, extremando las precauciones en el envío de *e-mails* externos a la organización y evitando hacer uso de medios cuya seguridad nos genere dudas.

- ✓ **Mantener al día las actualizaciones de seguridad** relativas a sistemas operativos, versiones del navegador de Internet y las extensiones y complementos. Si la persona trabajadora evita tener un software obsoleto, las probabilidades de sufrir ataques se reducen.

- ✓ **Fomentar un acceso cuidadoso a la información que está a disposición de la organización para llevar a cabo la actividad diaria.** EY considera que esta medida es especialmente relevante en la actualidad debido al auge del teletrabajo y donde tanto las empresas como los/as empleados/as tienen parte de responsabilidad:

  - Las **organizaciones** han de compatibilizar el uso de herramientas colaborativas con la protección y la seguridad de la información.

  - Los/as **trabajadores/as** deben evitar descargar o almacenar información corporativa en equipos personales.

- ✓ **Establecer reglas sólidas de seguridad y monitorizar los accesos y conexiones** para detectar cualquier actividad considerada extraña o perjudicial en materia de seguridad.

- ✓ **Gestionar adecuadamente las contraseñas**, haciendo que éstas sean largas y complejas. También se recomienda que sólo sean conocidas por el/la trabajador/a, que se cambien de manera frecuente y que no se reutilicen aquellas que ya se han utilizado anteriormente.

- ✓ **Contar con programas antivirus en todos los equipos y mantenerlos actualizados.**

- ✓ **Garantizar la seguridad en la conexión remota,** haciendo uso siempre que sea posible de una Red Privada Virtual (RPV). Si las conexiones se realizan desde casa, hay que asegurarse de que el acceso a la WIFI sea a través de una contraseña robusta. Además, es importante proteger con contraseña los envíos de archivos que contienen información sensible para la organización.

- ✓ **Evitar abrir correos y enlaces de origen desconocido, desconfiar de peticiones de datos personales o credenciales de acceso y descargar únicamente aplicaciones para el teléfono móvil a través de páginas web oficiales.** De este modo, se pueden evitar dos tipos de ataques dirigidos muy habituales:

  - **La infección con *malware*,** que puede conducir al control del ordenador de forma remota y al robo de información a través de un software espía.

  - **El *phishing* o *spear phishing*,** que permite la obtención sin autorización de credenciales de acceso a banca *online*, tarjetas de crédito, etc.

- ✓ **Asegurarse de la veracidad de la información recibida y evitar difundir información falsa.**

El dato

La implantación masiva del teletrabajo debido a la pandemia de la Covid-19 ha abierto nuevas brechas de seguridad en las empresas, como evidencian los datos del equipo de seguridad de IBM referentes al primer trimestre de 2020:

- ✓ A **nivel mundial**, la **cantidad de ataques informáticos aumentó en un 40%** en comparación con el mismo período del año anterior.
- ✓ En el caso de **Europa**, el aumento del número de ciberataques es aún más impactante, registrando un **crecimiento del 125%** respecto al año anterior.

Pero **no sólo el teletrabajo aumenta el riesgo de sufrir ciberataques**. Tanto si se trabaja en remoto como presencialmente, **es esencial el papel de los/as trabajadores/as**. Se ve reflejado en una investigación realizada por la Stanford University y la firma de ciberseguridad Tessian, que advierte que:

- ✓ La **fatiga** y el **estrés** de los/as profesionales repercuten directamente en la ciberseguridad. Esta cuestión es especialmente relevante teniendo en cuenta que **el 93% de las personas encuestadas reconoce sentir cansancio y estrés durante su jornada laboral.**

Guía de Trabajo

PRIMEROS PASOS PARA REDUCIR EL RIESGO DE SUFRIR CIBERATAQUES

Según el artículo *Medidas clave para garantizar la ciberseguridad en la empresa*, publicado en la web de la firma de servicios profesionales BDO, para evitar posibles ataques virtuales y mitigar los daños en caso de que éstos se produzcan, es fundamental que las organizaciones pongan el foco en la ciberseguridad:

- **Implementando acciones focalizadas en el cifrado de la información** y **realizando regularmente copias de seguridad.**
- **Desarrollando protocolos de actuación que permitan responder con agilidad en caso de ciberataque.** Para favorecer esta respuesta rápida, es fundamental organizar y jerarquizar previamente los datos para facilitar su rastreo.
- **Velando por el correcto cumplimiento de todos los protocolos y medidas:** es importante que las empresas lleven a cabo evaluaciones periódicas en todas sus áreas y departamentos. De este modo, se podrá garantizar una seguridad real.

LOS/AS PROFESIONALES: LA CLAVE PARA CONSEGUIR UN ENTORNO VIRTUAL SEGURO

El papel de las personas es básico a la hora de garantizar la seguridad en el entorno virtual. En consecuencia, es necesaria la implicación directa de la función de Personas a través de acciones como:

- **La identificación, atracción y retención de talento profesional:** es necesario que las organizaciones cuenten con profesionales cualificados, tanto ingenieros expertos en TI como otros perfiles, por ejemplo, politólogos o criminólogos. De esta manera, se podrá entender lo que hay detrás de cada ciberataque (motivación, modelo económico, perfil del atacante, etc.) y será posible mejorar la capacidad de respuesta.

- **La integración del talento cualificado a las estructuras corporativas:** es fundamental que los/as profesionales encargados/as de evitar cualquier ataque a los sistemas de información se sientan apoyados dentro de la organización y puedan trabajar con todas las facilidades posibles. Aún así, en muchas organizaciones, tal y como se expone en el artículo de Observatorio de Recursos Humanos *El déficit de talento en ciberseguridad incrementa los riesgos digitales de las empresas*, chocan con cierta falta de sensibilización corporativa y, además, trabajan con un presupuesto limitado y deben dedicar mucho tiempo a realizar tareas de cumplimiento normativo.

- **La concienciación y formación del conjunto de las personas empleadas en materia de ciberseguridad.**

La experiencia

ElTenedor es una plataforma fundada en 2007 a través de la cual se pueden efectuar reservas en restaurantes de forma gratuita y en tiempo real. La compañía, que desde el año 2014 forma parte de TripAdvisor Media Group, cuenta con unas 900 personas empleadas y opera en 17 países de todo el mundo. Uno de los principales éxitos de ElTenedor tiene que ver con la participación de los/as usuarios/as y la de los/as restauradores/as, ya que la aplicación recoge valoraciones e informaciones proporcionadas por todos/as ellos/as con el fin de facilitar la búsqueda del restaurante idóneo para cada momento.

- ✓ La plataforma lanzó una promoción conocida como "**The yummy days**", que consistía en un juego diario que permitía ganar durante una semana una comida gratis valorada en un máximo de 120 euros y varios premios en forma de *Yums*. Cabe destacar que los *Yums* son puntos que se obtienen al reservar a través de ElTenedor y que se pueden canjear por descuentos en los restaurantes asociados.

- ✓ Tal y como se explica en el artículo de Medium *An Ethical Hacking Story - The Yummy Days Case*, el ingeniero y desarrollador de aplicaciones web Héctor Martos detectó casi por casualidad un **problema de seguridad a nivel tecnológico** en esta promoción.

  - Para participar, era necesario rellenar un formulario donde se pedía el correo electrónico y se debían aceptar las condiciones de uso. Una vez realizado este paso y habiendo participado en el juego que proponía la plataforma, se podía saber si se había ganado algún premio o no. En una de las ocasiones en que el ingeniero rellenó el formulario, percibió que podía ver fácilmente la URL a la que estaba accediendo.

  - Gracias a sus conocimientos, observó que la interfaz del usuario estaba haciendo solicitudes a un servidor API. Decidió, pues, guardar las solicitudes y respuestas e intentó jugar nuevamente introduciendo su correo electrónico. No fue posible, ya que se le redirigía a una página que especificaba que ya había participado anteriormente. Sin embargo, sí que pudo participar con otra dirección de correo no registrada en la aplicación de ElTenedor. Según explica el propio ingeniero, "la API no validaba si el correo introducido estaba registrado en la aplicación o no". Así pues, podía jugar una y otra vez con direcciones diferentes para intentar ganar más premios.

  - Esta no es una problemática especialmente grave si pensamos en una persona que participa repetidamente en la promoción introduciendo manualmente diferentes *mails*. Según el desarrollador de aplicaciones web, el verdadero problema de seguridad para la plataforma tiene que ver con la posibilidad de automatizar este proceso y repetirlo cada segundo. Héctor Martos decidió ponerlo en práctica y demostrar que podía ganar varios premios de forma automática. Lo consiguió y, posteriormente, informó a la plataforma para que pudieran solucionar la vulnerabilidad detectada.

- ✓ Hay que tener en cuenta que si el ingeniero no hubiera notificado el problema y más participantes hubieran detectado esta vulnerabilidad, se habría puesto en entredicho la **seguridad** de la plataforma, lo que habría podido afectar negativamente a la **reputación del negocio.**

Charter of Trust es una iniciativa impulsada por la multinacional alemana Siemens que ha logrado unir los esfuerzos de 16 empresas más, que operan a nivel internacional y en múltiples sectores, con el propósito de lograr un entorno digital más seguro. Esta iniciativa surgió en el marco de la Conferencia de Seguridad de Munich del año 2018 con el fin de "proteger los datos de particulares y empresas, prevenir daños a personas, organizaciones e infraestructuras y crear unos cimientos fiables sobre los cuales la confianza en la Red pueda crecer", tal y como exponen desde su propia página web. Entre los firmantes de la carta destacan empresas como Airbus, Allianz, IBM, Atos y Mitsubishi Heavy Industries, entre otras.

- ✓ En los últimos meses el teletrabajo se ha convertido en una opción laboral utilizada de forma masiva debido a la pandemia de coronavirus y ha sido necesario poner el foco en la **ciberseguridad**, ya que la fiabilidad y seguridad de los entornos virtuales trabajando desde casa no es la misma que desde las oficinas y los *hackers* pueden aprovechar este tipo de vulnerabilidades. Por ello, la iniciativa Charter of Trust ha dado a conocer 8 consejos que deben permitir **mantener la actividad habitual de los negocios mientras se trabaja *online*** y, al mismo tiempo, **prevenir posibles ciberataques.**

  - **Recomendaciones de los socios de Charter of Trust,** que se pueden consultar a través de su página web:

    - ❖ Llevarse a casa sólo aquellos dispositivos que son imprescindibles y consultar y utilizar sólo la información necesaria.
    - ❖ Mantener el software actualizado en todos los dispositivos.
    - ❖ Optar sólo por comunicarse de forma segura y protegiendo la red doméstica.
    - ❖ Utilizar los dispositivos de uso empresarial sólo para la realización de la actividad laboral y reservar la utilización de los dispositivos personales para el uso no profesional.
    - ❖ Apagar los dispositivos inteligentes controlados por voz que se encuentran en el entorno de trabajo y cubrir la cámara web cuando no está en uso.
    - ❖ Identificar proactivamente a las personas participantes en las reuniones realizadas por videollamada.

- Cerrar la sesión cuando el dispositivo no está en uso y guardarlo de forma segura.
- Tener especial cuidado al abrir correos electrónicos y archivos adjuntos que puedan considerarse sospechosos, sobre todo si no se conoce al remitente.

Materiales

Bibliografía básica

Arreola, Adolfo. *Ciberseguridad: ¿Por qué es importante para todos?* Barcelona: Siglo Veintiuno editores, 2019

Dans, Enrique. *Viviendo en el futuro. Claves sobre cómo la tecnología está cambiando nuestro mundo.* Bilbao: Deusto, 2010

Stephens-Davidowitz, Seth. *Todo el mundo miente. Lo que Internet y el Big Data pueden decirnos de nosotros mismos.* Madrid: Capitán Swing, 2019

Materiales en línea

Ciberseguridad en el teletrabajo: Una guía de aproximación para el empresario

Guía elaborada por el Instituto Nacional de Ciberseguridad (Incibe) con el objetivo de ayudar a las organizaciones a garantizar el acceso seguro de los/as trabajadores/as a los sistemas de información de la empresa mientras trabajan en remoto. En este documento se exponen los principales riesgos del teletrabajo en materia de ciberseguridad y, además, se recogen algunas recomendaciones y medidas para proteger la información.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

Doménech, Enric. "Medidas clave para garantizar la ciberseguridad en la empresa". *BDO España*, 22/11/2019.

Artículo de la firma de servicios profesionales BDO que recoge un total de 9 medidas preventivas que tienen como objetivo reducir el riesgo de sufrir ciberataques o, al menos, minimizar los daños causados por la apropiación indebida de información y de datos.

https://www.bdo.es/es-es/publicaciones/articulos/medidas-para-garantizar-la-ciberseguridad

Kit de concienciación para empresas, del Instituto Nacional de Ciberseguridad (Incibe)

Recursos didácticos y herramientas de entrenamiento que el Instituto Nacional de Ciberseguridad (Incibe) pone a disposición de las organizaciones, especialmente de las pymes y las microempresas, para facilitar la concienciación y la formación de sus plantillas en materia de ciberseguridad. Este kit es aplicable a empresas de todos los sectores y sin necesidad de tener conocimientos técnicos previos.

https://www.incibe.es/protege-tu-empresa/kit-concienciacion

Unidades de Conocimiento relacionadas

- Teletrabajo (2020): https://factorhuma.org/es/unidades-de-conocimiento-blog/14574-teletrabajo
- Adaptación a la nueva Ley de Protección de Datos (2018): https://factorhuma.org/es/unidades-de-conocimiento-blog/13746-adaptacio-a-la-nova-llei-de-proteccio-de-dades