Fortaleciendo la Resiliencia Digital: Estrategias de Ciberseguridad para los Contadores de las Américas desde el Aula Virtual de AIC

Autora: Yvonne Luzette Huertas
Presidenta Comisión Técnica de Sistemas y TI

En el mundo digital de hoy, la ciberseguridad se ha convertido en una prioridad crítica para las empresas de todos los sectores, sin importar lo grande o pequeña que pueda ser. La creciente dependencia de la tecnología y la interconexión global han expuesto a las organizaciones a una variedad de amenazas cibernéticas que pueden comprometer la integridad, confidencialidad y disponibilidad de la información. Los ataques cibernéticos no solo pueden causar pérdidas financieras significativas, sino también dañar la reputación de una empresa y erosionar la confianza de sus clientes. Son pérdidas irreparables que hay que evitar a toda costa o por lo menos estar preparados para mitigar el impacto de ellas.

Como contadores y auditores, desempeñamos un papel fundamental en la protección de la información sensible y en la implementación de controles efectivos para mitigar los riesgos cibernéticos. Hoy más que nunca los “stakeholders” confían ejerceremos nuestros mejores oficios como consejeros de confianza. Nuestra responsabilidad va más allá de los números; debemos asegurarnos de que los sistemas y procesos que manejan datos financieros y personales estén protegidos contra accesos no autorizados y ataques maliciosos.

Te invito a unirte a nuestra aula virtual, donde exploraremos un caso real de ciberseguridad en empresas de América Latina. Hemos cambiado nombres, países, y otros detalles para asegurar la protección de datos y cumplir con la confidencialidad requerida. A través de este caso, analizaremos las vulnerabilidades y fortalezas, y aprenderemos cómo implementar medidas efectivas para mitigar los riesgos. Este caso está diseñado para proporcionar una visión práctica y detallada de los desafíos de ciberseguridad que enfrentan las empresas hoy en día, y cómo podemos abordarlos de manera proactiva.

En este recorrido, te convertirás en un participante activo, analizando datos, identificando problemas y proponiendo soluciones. Al final de esta experiencia, no solo habrás adquirido conocimientos valiosos sobre ciberseguridad, sino que también estarás mejor preparado para proteger tu organización contra las amenazas cibernéticas.

¡Bienvenido a esta aventura educativa y transformadora!

Caso 1: Empresa de Servicios Financieros

En el corazón de la Ciudad de México, Financieros Unidos Innovadores S.A. se erige como un coloso en el mercado financiero mexicano, con sucursales en Monterrey, Guadalajara, Puebla y Tijuana. Esta entidad ofrece una amplia gama de servicios financieros, desde la gestión de inversiones hasta la banca corporativa, siendo una fortaleza de confianza para sus clientes.

Sin embargo, recientemente, la empresa se ha visto envuelta en una sombría tormenta de intentos de phishing. Emails fraudulentos, disfrazados de comunicaciones legítimas de la propia empresa o de instituciones financieras respetadas, han comenzado a invadir las bandejas de entrada de sus empleados. Su objetivo: engañar a estos desprevenidos trabajadores para que revelen información confidencial, como contraseñas y datos de clientes, o para que hagan clic en enlaces que descargan malware en sus dispositivos.

Laura, una contadora senior con más de una década de experiencia en la empresa, y Carlos, un meticuloso auditor interno, han sido identificados como empleados que utilizan sus dispositivos personales para acceder a sistemas críticos de la empresa. Estos dispositivos personales, lamentablemente, carecen de las medidas de seguridad adecuadas, como software antivirus actualizado, firewalls y autenticación multifactorial, lo que incrementa alarmantemente el riesgo de brechas de seguridad.

Además, se ha destapado un inquietante secreto: la empresa no cuenta con un programa de capacitación en ciberseguridad para sus empleados. Muchos de ellos desconocen las mejores prácticas para identificar y evitar ataques de phishing, así como la protección adecuada de la información confidencial de la empresa. Esta carencia de formación deja a la empresa expuesta a una amplia gama de amenazas cibernéticas, poniendo en jaque la integridad de la información financiera y la continuidad del negocio.

Al analizar estos datos, debemos ponernos en los zapatos de un contador que realiza una radiografía minuciosa de la situación. Como profesionales de la contabilidad, nuestra labor va más allá de los números; debemos considerar también los riesgos operativos y de seguridad que pueden comprometer la integridad de la información y la continuidad del negocio. Este análisis detallado nos permitirá identificar las áreas críticas que requieren atención inmediata y desarrollar estrategias efectivas para fortalecer la postura de ciberseguridad de la empresa.

A continuación, procederemos a desentrañar las vulnerabilidades generales y específicas detectadas en este caso, y ofreceremos recomendaciones prácticas para mitigar estos riesgos.

Nuestra primera recomendación: prepara una lista de preguntas claves para identificar los retos y riesgos relacionados a la ciberseguridad de la empresa:

Preguntas Clave para el Análisis del Caso:

1. Identificación de Amenazas
    - ¿Cuáles son los tipos de intentos de phishing detectados?
    - ¿Qué métodos están utilizando los atacantes para engañar a los empleados?
2. Evaluación de Vulnerabilidades
    - ¿Qué dispositivos personales están siendo utilizados por los empleados para acceder a sistemas críticos?
    - ¿Qué medidas de seguridad faltan en estos dispositivos personales?
    - ¿Qué vulnerabilidades específicas se han identificado en los sistemas de la empresa?
    - ¿Es la política de la empresa permitir que los empleados usen dispositivos personales?
3. Impacto en la Empresa
    - ¿Qué información confidencial está en riesgo debido a estos intentos de phishing?
    - ¿Cómo podrían estas brechas de seguridad afectar la integridad de la información financiera?
    - ¿Cuál es el impacto potencial que el ataque cibernético tiene en la continuidad del negocio?

4. Capacitación y Concienciación
    - ¿Existen protocolos en las entrevistas de reclutamiento de personal para asegurar la integridad profesional de quienes ingresan como empleados de la empresa?
    - ¿Tiene la empresa un código de ética vigente que provea normas en cuanto a la conducta con sistemas de tecnologías?
    - ¿Qué nivel de conocimiento tienen los empleados sobre ciberseguridad?
    - ¿Qué tipo de programa de capacitación en ciberseguridad sería más efectivo para la empresa?
    - ¿Cómo se puede mejorar la concienciación sobre ciberseguridad entre los empleados?
5. Medidas de Mitigación
    - ¿Qué medidas inmediatas se pueden tomar para proteger los sistemas críticos?
    - ¿Qué políticas de uso de dispositivos personales se deben implementar?
    - ¿Qué tecnologías de seguridad adicionales se deben considerar (por ejemplo, autenticación multifactorial, cifrado de datos)?
6. Estrategias a Largo Plazo
    - ¿Cómo se puede desarrollar un programa integral de ciberseguridad para la empresa?
    - ¿Qué pasos se deben seguir para mantener la seguridad a largo plazo?
    - ¿Cómo se puede evaluar y actualizar continuamente las políticas y procedimientos de ciberseguridad?

Nuestra segunda recomendación: Has la radiografía de la situación con un análisis general y análisis específico.

Análisis General

A primera vista, se detectan varias vulnerabilidades en esta empresa. No existe un plan de capacitación en ciberseguridad para los empleados. Además, se observa que, probablemente como resultado de las medidas implementadas durante la pandemia de COVID-19, aún se permite el uso de dispositivos personales. Un aspecto que inmediatamente captura nuestra atención es el aumento significativo en los intentos de phishing.

La empresa enfrenta un riesgo significativo debido a la falta de capacitación en ciberseguridad y al uso de dispositivos personales no seguros. Los intentos de phishing son una amenaza común que puede tener consecuencias graves si no se abordan adecuadamente.

No todo es negativo en el análisis de esta empresa. La presencia de la empresa en varias ciudades de México puede considerarse una fortaleza, ya que facilita la implementación de políticas de ciberseguridad a gran escala y potencia su capacidad para invertir en tecnologías de seguridad avanzadas. Esta amplia presencia geográfica también permite una mayor colaboración y coordinación entre las diferentes sucursales, lo que puede resultar en una respuesta más rápida y efectiva ante incidentes de seguridad. Además, la diversidad de ubicaciones puede proporcionar una mayor resiliencia operativa, permitiendo que la empresa mantenga sus operaciones incluso si una sucursal se ve comprometida. Aprovechando estas ventajas, la empresa puede establecer un equipo centralizado de ciberseguridad que supervise y coordine las iniciativas de seguridad en todas las ubicaciones, asegurando una protección uniforme y robusta en toda la organización.

Análisis Específico

1. **Intentos de Phishing**
    - **Descripción**: Se ha observado un aumento en los intentos de phishing dirigidos a los empleados, con correos electrónicos fraudulentos que buscan obtener información confidencial o inducir a los empleados a hacer clic en enlaces maliciosos.
    - **Impacto**: Riesgo de divulgación de información confidencial, comprometiendo la seguridad de los datos financieros y personales de los clientes.
2. **Uso de Dispositivos Personales**
    - **Descripción**: Empleados como Laura y Carlos están utilizando dispositivos personales para acceder a sistemas críticos sin las medidas de seguridad adecuadas.
    - **Impacto**: Aumento del riesgo de brechas de seguridad debido a la falta de control sobre los dispositivos personales y la posible presencia de malware.
3. **Falta de Capacitación en Ciberseguridad**
    - **Descripción**: La empresa carece de un programa de capacitación en ciberseguridad para sus empleados, lo que deja a muchos de ellos vulnerables a ataques de phishing y otras amenazas cibernéticas.
    - **Impacto**: Mayor susceptibilidad a ataques cibernéticos debido a la falta de conocimiento y concienciación sobre prácticas seguras.

Nuestra tercera recomendación: Procede a ofrecer recomendaciones prácticas para mitigar el riesgo de un ciberataque:

Recomendaciones Prácticas

- **Implementación de Políticas de Seguridad**: Desarrollar y aplicar políticas claras sobre el uso de dispositivos personales y acceso a sistemas críticos.
- **Capacitación Continua:** Establecer un programa de capacitación en ciberseguridad para todos los empleados, con actualizaciones regulares.
- **Tecnologías de Seguridad**: Adoptar tecnologías avanzadas de seguridad, como la autenticación multifactorial y el cifrado de datos, para proteger la información confidencial.
- **Monitoreo y Evaluación:** Implementar sistemas de monitoreo continuo para detectar y responder rápidamente a cualquier intento de brecha de seguridad.

Antes de concluir este artículo, es fundamental destacar que la ciberseguridad es un tema que nos afecta a todos. Es posible que en su empresa la concienciación sobre ciberseguridad no sea una prioridad alta. Sin embargo, desarrollar un plan de protección contra ciberataques no tendrá valor si el personal no le da la importancia que merece.

Entonces, ¿cómo podemos fomentar la concienciación sobre la importancia de mantener activo un plan de protección contra ciberataques?

1. **Importancia de la Ciberseguridad**: Comienza explicando por qué la ciberseguridad es crucial para las empresas, especialmente en el sector financiero.
2. **Problemas Actuales**: Menciona la falta de concienciación como uno de los principales problemas que enfrentan las organizaciones hoy en día.

3. **Identificación del Problema**:
    a) **Amenazas Comunes**: Describe las amenazas más comunes, como el phishing, el ransomware y otras formas de ataques cibernéticos.
    b) **Impacto de la Falta de Concienciación**: Explica cómo la falta de formación y concienciación puede convertir a los empleados en el eslabón más débil de la cadena de seguridad.
4. **Evaluación de Necesidades**: Realiza una evaluación de las necesidades de ciberseguridad en la organización. Identifica las áreas de mayor riesgo y las vulnerabilidades más comunes.
5. **Estrategias para Mejorar la Concienciación:**
    a) Programas de Capacitación Continua
    b) Contenido Relevante: Asegúrate de que los programas de capacitación incluyan información actualizada sobre las últimas amenazas y mejores prácticas.
    c) Frecuencia y Actualización: La formación debe ser continua y adaptarse a las nuevas amenazas.
    d) Involucrar a la Alta Dirección
    e) Liderazgo y Compromiso: La alta dirección debe estar comprometida y participar activamente en las iniciativas de ciberseguridad.
    f) Campañas de Concienciación - Mensajes Clave: Utiliza campañas de concienciación para recordar a los empleados la importancia de la ciberseguridad y las prácticas seguras.
6. **Herramientas y Recursos**: Proporciona herramientas y recursos, como guías y seminarios web, para educar a los empleados.
7. **Simulaciones de Ataques** - **Phishing Simulado**: Realiza simulaciones de ataques de phishing para evaluar y mejorar la capacidad de los empleados para identificar correos electrónicos fraudulentos.
8. **Políticas y Procedimientos Claros:**
    a. Uso de Dispositivos Personales: Implementa políticas claras sobre el uso de dispositivos personales y acceso a sistemas críticos.
    b. Autenticación Multifactorial: Promueve el uso de autenticación multifactorial y otras medidas de seguridad avanzadas.

Por si no tienes claro cuáles son los beneficios de una buena concienciación en Ciberseguridad, aquí te comparto algunos:

a. Protección de Datos Sensibles: Los empleados bien informados son más cuidadosos al manejar y compartir información confidencial.
b. Reducción de Incidentes: Una cultura de ciberseguridad efectiva reduce la probabilidad de éxito de los ataques cibernéticos.
c. Mejora de la Reputación: Demuestra el compromiso de la organización con la protección de los datos de sus clientes y socios comerciales.

Conclusión:

En resumen, la profesión contable enfrenta un panorama en constante evolución, impulsado por los avances tecnológicos y los nuevos desafíos globales. Las tecnologías que nos protegen de potenciales ataques cibernéticos deben ser exhaustivamente estudiadas por los contadores de las Américas. El componente ético debe siempre ser parte integral de la discusión, para asegurar que la rectitud, la integridad y la conducta intachable se mantengan en el ADN del contador.

Es imperativo reconocer que las amenazas no solo provienen del exterior; a veces, el “enemigo” puede estar dentro de nuestras propias filas. Esto resalta la necesidad de que los profesionales dentro de la empresa no solo sean éticos y ágiles en el manejo de las tecnologías, sino que también comprendan y apliquen adecuadamente las medidas de protección. La formación continua en ciberseguridad y ética es esencial para mitigar estos riesgos internos.

Es imperativo que los profesionales contables se mantengan actualizados y adopten un enfoque proactivo para integrar las mejores prácticas de ciberseguridad en su trabajo diario. La Asociación Interamericana de Contabilidad tiene un rol vital en fomentar la colaboración y el intercambio de conocimientos a nivel interamericano. Esto no solo enriquecerá nuestra profesión, sino que también fortalecerá nuestra capacidad para enfrentar los retos del futuro con integridad y excelencia. A través de la innovación y el compromiso continuo con la educación en áreas como la ciberseguridad y la ética, la Asociación Interamericana de Contabilidad puede asegurar que la contabilidad siga siendo una piedra angular en el desarrollo económico y financiero de nuestras sociedades.