Eficiencia en el gobierno y gestión del compliance en ciberseguridad

Juan Fco. Cornago Baratech
jcornago@sia.es
Ciber Risk & Compliance
DIGITAL RISK

ISACA Madrid Chapter

Índice

1. RETO:
Explicar qué es el COVID-19 a un niño

La epidemia del **COVID-19** ha provocado que **millones de niños** no puedan ir al colegio, hacer deporte o realizar cualquier tipo de actividad extraescolar.

Al pasar más tiempo del habitual en sus casas, los **niños** están constantemente **escuchando noticias** entorno al **virus** y sus efectos.

El **reto** es **saber comunicar a los niños cómo afrontar el virus**.

OBJETIVO:
Lograr una seguridad Integrada y eficiente

La **convulsa actualidad** que nos asiste desde hace unos años, en el ámbito de la **ciberseguridad**, ha **creado** un **clima** de **miedo** y **frustración** constante.

No importa cuánto trabajes que la sensación de **no disponer de recursos suficientes** para luchar es común en todas las Organizaciones.

Nuestro **objetivo** es **implantar un sistema de Seguridad Integral y eficiente.**

2. ¿Qué conocimiento tiene el niño de la situación?

- Lo fundamental es **escuchar** a los niños sobre lo que **creen saber** de la enfermedad.
- Es **importante no minimizar** sus **preocupaciones** o miedos.
- Debemos **recordarles que pueden preguntar todo lo que necesiten** saber en cualquier momento.
- Puedes **utilizar dibujos o cuentos** para que empiecen a hablar.

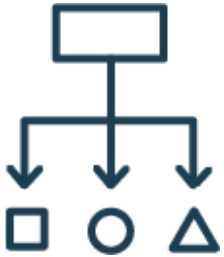
¿Cuáles son las normativas y buenas prácticas que ayudan?

- **Conocer normas** y aspectos legales que **aplican**.
- **Desarrollar** un **Modelo Unificado de Controles (MUC)** donde encuentres el Máximo Común Divisor de los **controles aplicables**.
- **Crear un Sistema Integrado de Gestión (SIG)** que permita **organizar** los **procesos** de seguridad en toda la Organización.

3. Hay que ser realistas

- Los niños tienen **derecho a saber** la **realidad** y estar informados. Somos los adultos quienes debemos ayudarlos a superar la tristeza.
- **No te inventes nada** que no sepas. Busca información y sé crítico.
- **Cuidado con las Fake News y los bulos**. Los niños deben saber que no todo lo que se dice es verdad.

Seguridad basada en el riesgo



- La base de cualquier estrategia es el **conocimiento** de la **situación**. Necesitas una **Metodología de Análisis de Riesgos Ágil** (**MARA**) para ahorrar tiempo.
- Todas las **medidas** que se tomen **deben** estar basadas en la **mitigación** de **estos riesgos**.
- **No** existen **remedios para todos**, cada uno tiene sus propios problemas.

4. Aprender a protegerse

- La forma de **concienciar** a los niños es fundamental a la hora de conseguir el objetivo. **Jugar** a lavarse las manos con canciones y cuentos es la manera más adecuada.
- **Hay que enseñarles** cómo toser y estornudar para no contagiar a otros niños así como mantener la distancia.
- **Deben avisar** en caso de que se encuentren con síntomas.

Planes de concienciación

- Los neurocientíficos creen que el **ser humano toma** más **decisiones** con los **sentimientos** que con la razón.
- La mejor forma de **concienciar** es **persuadiendo** a las **personas** para que **tomen** las **decisiones** más **seguras** para la protección de la información.
- Es **fundamental** tener **canales abiertos** para que los usuarios puedan **reportar incidentes y evaluar acciones.**

5. Seguridad ante todo

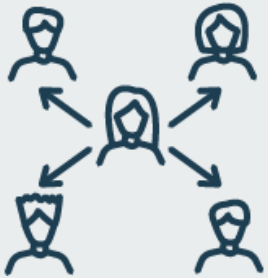
- El entorno social puede crear una situación de alarma y miedo descontrolado en los niños. Es fundamental **mantener rutinas** con los niños.
- **En caso de brote** en el entorno es fundamental hacerles ver que **lo más probable** es que **no se contagien** y que hay muchas personas trabajando para evitar que le pase nada.

Medir es la base de la información

- Los **procedimientos e instrucciones técnicas** bien definidos y ejecutados son la **base** para **mantener** unas **defensas bien** implantadas.
- La **constante medición** del estado de implantación, **y** en su caso **gestión de la no conformidad**, son la **base** para que la **Dirección** de la organización **sepa** qué se está haciendo.

6. Combatir discriminación

- La **situaciones de estrés** pueden generar **comportamientos** en los niños **inadecuados**, como son la **discriminación** y o **amenazas** a otros niños. Es importante que los **adultos estén al tanto** de los niños para **evitar** estas situaciones.
- El **acoso** es una **conducta inadecuada. Debemos enseñar** a los niños a **ayudar** a los demás.



No todo es seguridad, la continuidad es el objetivo

- **En** momentos de **crisis no podemos** hacer que la **seguridad frene** el **negocio**. Pero para evitar problemas, debemos **generar planes de continuidad seguros y bien probados.**
- La **continuidad** es el **área** más **cercana al negocio, debes cuidarla.**
- Los **planes de continuidad deben ser seguros, automáticos y estar basados** en la correcta **formación** al usuario.

7. Ayuda externa

- No todo son malas noticias con el COVID19, también hemos visto cómo **afloran los sentimientos de bondad y ayuda** de las personas ayudándose unas a otras. Este **es un mensaje muy bueno para transmitir a los niños.**
- **Contar** a las niños las **historias** de **médicos**, **enfermeros**, **voluntarios**, **policías**, etc. **le ayudará** mucho.

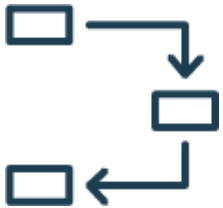
Servicios en la nube

- Las **soluciones en la nube**, de forma **segura e integradas con las Organizaciones**, **son una ayuda** para las áreas de explotación de las compañías.
- Independientemente del modelo elegido, **nunca** debes **perder** el **proceso** de **GRC** del **sistema ni** el **control del dato**.
- **Utiliza estándares** como la **ISO 27017, STAR ,AENOR, Leet Security, etc. en proveedores** y **clientes**.

8. Cuídate

- **Para ayudar** a los niños, **primero debes cuidarte tú mismo**. Tu **forma de actuar y obrar** será el mejor **ejemplo** que los niños seguirán.
- **Debes saber cómo actuar** ante las situaciones cotidianas.
- Los **adultos deben encontrar actividades que les permitan relajarse y recuperarse**, pues esta enfermedad permanecerá muchos meses más.

Planes de Acción



- **Sabiendo** las **medidas concretas** que mitigan el riesgo específico de la Organización, **elaboramos** los **planes de acción más adecuados a cada organización**.
- Utiliza **metodología basadas en el Ciclo de Vida del Control (CVC)** que permitan **entrelazar** el ciclo de vida de la medida **con** los **actores internos** que deben intervenir.

9. Prudencia

- Los niños **no se deben quedar angustiados** tras la conversación. **Debemos medir su grado de ansiedad** a través del **lenguaje no verbal.**
- Los niños **seguirán preguntando**, a veces sobre lo mismo, para lograr entender bien lo que pasa. Los **adultos deber ser pacientes y estar disponibles.**

Cambio cultural

- Uno de los aspectos que más se cuidad en los proyectos de concienciación es la **medición**, en todo momento, y **por diferentes vías**, del **impacto** que se genera **en los usuarios** del plan.
- La **concienciación** ya **no** es algo **exclusivo** y dedicado a los **trabajadores**, sino que **debemos exteriorizarlo** al **resto** de la **sociedad**.

10. Beneficios

Planes y acciones personalizadas, adaptadas a las necesidades y características de la organización.

Mejora de la imagen de la seguridad, más cercana y accesible a los empleados y a sus familiares.

Aumento del grado de implicación y motivación de los empleados en protección de la información.

Implantación de una **cultura de seguridad más persistente** en la organización.

Incremento del cumplimiento legislativo y de estándares internacionales en materia de seguridad (RGPD, ENS, ISO 27001, ISO 22301, etc.).

Disminución del riesgo de incidentes de seguridad y mejora de su gestión.

Gracias

ISACA
Madrid Chapter