Cómo implementar una estrategia de ciberseguridad empresarial:

Entrevistas Axity

La ciberseguridad no es un tema que se debe tomar a la ligera en ningún aspecto, ni a nivel personal y mucho menos empresarial, pero este último presenta unos riesgos complejos debido a que grandes sumas de dinero y datos sensibles están en juego si no se cuenta con la protección suficiente.

No sólo evoluciona la tecnología con intenciones positivas y productivas, esta capacidad de invención, creación y cambio también la tiene el cibercrímen y debemos estar preparados.

Mucho hemos escuchado de este tema, pero pocas veces **tenemos la oportunidad de contar con un experto que nos hable en detalle sobre los pasos necesarios para que nuestras organizaciones cuenten con el nivel de prevención, protección y reacción** necesario para enfrentarse a la cantidad inagotable de amenazas que surgen cada día.

Por eso, en este ebook entrevistamos a Hensy Hernández, gerente de Ciberseguridad en Axity. Desde su experiencia y conocimiento, expuso las claves para tomar acción y estar preparados ante los riesgos cibernéticos.

¡Empieza a explorar!

ÍNDICE

Da click en el ÍTEM de tu interés

1 Roles definidos = decisiones efectivas

- ¿Qué importancia tiene esta delegación de roles de gestión en la estructura de gobierno de ciberseguridad?
- ¿Cómo afecta el fortalecimiento del nivel de madurez de una empresa?

2 Presupuesto e inversión en ciberseguridad

- ¿Qué relación existe entre el tamaño del presupuesto que se debe invertir en ciberseguridad con el nivel de riesgos que tiene la organización?
- ¿Cómo afecta el nivel de crecimiento potencial o de madurez de una empresa en el presupuesto que se debe invertir?

3 Integración de soluciones en la gestión empresarial

- ¿Cómo funciona esta integración de gestión de ciberseguridad con otros procesos clave de la organización?
- ¿Cómo garantizar el correcto desarrollo, monitoreo y entendimiento de esta integración?

4 Tercerización de la ciberseguridad, una estrategia empresarial

- ¿Qué factores debe tener en cuenta una empresa para tomar esta decisión de tercerización y cuáles son las ventajas que pueden salir de esto?
- ¿Cómo definir una estrategia junto a los proveedores expertos de soluciones tecnológicas que cubra en su totalidad las necesidades de cada organización?

5 El activo principal: la información

- ¿Con cuáles tipos de tecnologías destinadas a la protección de la información y de sus sistemas contra amenazas debe contar cada entidad?
- ¿Cuál es el alcance de las capacidades de estas tecnologías de detección y protección?

6 Ataques de negación de servicio (DDoS) en auge

- ¿Qué tipo de optimización y actualización de herramientas para la protección de DDoS se debe implementar en las organizaciones para reducir los riesgos de estos ataques?

7 Inteligencia ante las amenazas: monitoreo 24/7

- ¿Cómo se realiza este proceso de recolección, almacenamiento, divulgación y concientización de esta información?
- ¿Cómo generar un análisis de inteligencia de amenazas y procesos de preparación y respuesta óptimos?

1 Roles definidos = decisiones efectivas

Empecemos hablando de la gestión de responsabilidades que cada empresa debe tener en su política de ciberseguridad. La estipulación de roles claros y definidos permite una toma de decisiones más efectiva y con visión a resultados futuros. Sobre este primer paso,

Entrevistador

¿Qué importancia tiene esta delegación de roles de gestión en la estructura de gobierno de ciberseguridad y cómo esto afecta el fortalecimiento del nivel de madurez de una empresa?

Experto Axity

Para iniciar, es necesario comprender que **la ciberseguridad no solo es una responsabilidad de un grupo especialista en el tema, sino que involucra a todos los actores y colaboradores de las empresas,** desde sus diferentes roles y áreas. Pero no solo eso, las compañías que buscan o desean tener un gobierno de ciberseguridad maduro, deben contar con políticas, procesos, procedimientos, planes, roles y responsabilidades acorde a esa madurez que se propone alcanzar.

Una vez se definen las políticas y procedimientos, **los roles de cada persona servirán para establecer, coordinar y organizar las responsabilidades dentro del programa de ciberseguridad,** así como los planes que se definan. Este trabajo colaborativo permitirá avanzar en esa hoja de ruta a la madurez.

volver al índice

2 Presupuesto e inversión en ciberseguridad

La preocupación por el presupuesto que se debe invertir en estas soluciones de ciberseguridad es un tema latente que interesa a todas las empresas en todo momento.

Entrevistador

¿Qué relación existe entre el tamaño del presupuesto que se debe invertir en ciberseguridad con el nivel de riesgos que tienen la organización?

¿Es directamente proporcional?

Y dentro del mismo tema, ¿cómo afecta el nivel de crecimiento potencial o de madurez de una empresa en el presupuesto que se debe invertir?

Experto Axity

Podríamos decir que la relación es directamente proporcional. **Al existir mayor riesgo en el negocio, debo invertir más en los controles de protección para gestionar esos riesgos que existen.** Lo que no se puede determinar a priori es la inversión exacta que se debe hacer, pues depende de un análisis de riesgos, la madurez a la que se quiere llegar y los planes que se vayan a ejecutar.

El análisis de riesgos es fundamental, ya que es el que nos dice exactamente qué riesgos hay y dónde ubicar los controles, evitando así que se invierta en puntos de bajo riesgo y se deje de invertir donde hay información o transacciones que requieren mayor control de seguridad.

Sabías que...

Según la **Encuesta de Riesgo Cibernético en tiempos de COVID19 en Latinoamérica,** realizada en agosto de 2020 por Marsh y Microsoft:

El **23%** de los encuestados han incrementado su percepción frente a la importancia de invertir en uno de estos seguros.

El **17%** de las entidades cuentan con un seguro de riesgo cibernético.

volver al índice

3 Integración de soluciones en la gestión empresarial

Sabemos que todas las piezas que integran una organización deben estar en continua sincronía para que cada uno de sus elementos funcione de manera óptima, por eso, el tema de la integración de las soluciones de ciberseguridad con el resto de gestiones empresariales es un paso fundamental.

Entrevistador

¿Cómo funciona esta integración de gestión de ciberseguridad con otros procesos clave de la organización?

¿Cómo garantizar el correcto desarrollo, monitoreo y entendimiento de esta integración?

Experto Axity

La ciberseguridad y seguridad de la información son componentes esenciales para cualquier compañía y como tal deben estar sincronizados e integrados en todos los demás procesos que tenga la organización. En ocasiones, dichos procesos o equipos de seguridad pueden verse como obstáculos o stoppers para la ejecución de proyectos y actividades.

De ahí la importancia de saber sincronizar las exigencias y actividades que se desarrollan para cumplir la seguridad, sin que estas detengan el buen funcionamiento del equilibrio. Para lograrlo, **es necesario hallar un equilibrio entre las operaciones del negocio y el cumplimiento de los controles de seguridad.**

Inicia desde una dirección general, con la convicción y conciencia de que el negocio debe funcionar con las medidas de seguridad adecuadas. De este modo, la dirección va a hacer (y ese es el reto) que sus equipos de trabajo se integren de la forma adecuada, para que todas sus operaciones funcionen, pero aplicándoles las medidas de seguridad que se necesitan y que han sido evaluadas según los riesgos del negocio.

3

Entrevistador

¿Cómo funciona esta integración de gestión de ciberseguridad con otros procesos clave de la organización?

¿Cómo garantizar el correcto desarrollo, monitoreo y entendimiento de esta integración?

Experto Axity

Cabe resaltar que la integración no solo se debe dar en las directivas y personal estratégico de la organización. **Todos los componentes deben trabajar en sincronía para lograr los resultados esperados: personas, procesos y tecnología. Su interacción en todos los niveles de la organización será indispensable.**

Las personas como componente principal cumplen un rol decisivo en la gestión de la seguridad y deben integrarse a las políticas de seguridad existentes en la organización. Como parte de ese compromiso, es clave que el colaborador propenda por aplicar controles de seguridad en las labores que realiza tanto dentro como fuera de la organización.

Por ejemplo, el teletrabajo y trabajo remoto se ha incrementado a raíz de la pandemia y "como cualquier gran cambio en tecnología" conlleva riesgos. **El reto es poder mantener la seguridad aun cuando cambie la manera de acceder a la información.** Por esa razón los trabajadores remotos también deben integrarse a los procesos y a las políticas definidas por la organización para ejecutar sus actividades de la manera más segura.

Sabías que...

Según un informe de INTERPOL durante la pandemia, y en solo un cuatrimestre (entre enero y abril) del 2020, hubo un **incremento alarmante en los ataques cibernéticos** a raíz del trabajo remoto y en casa. Por ejemplo, aumentó:

volver al índice

4

Tercerización de la ciberseguridad, una estrategia empresarial

Hablemos ahora sobre la utilización de servicios gestionados y la tercerización como estrategia para complementar las capacidades de ciberseguridad. Debido a la disponibilidad de recursos humanos de cada empresa y a la complejidad de la gestión de seguridad de la información, muchas organizaciones recurren a terceros para el manejo de estos procesos.

Entrevistador

¿Qué factores debe tener en cuenta una empresa para tomar esta decisión de tercerización y cuáles son las ventajas que pueden salir de esto?

Experto Axity

A la hora de gestionar la seguridad, **la tercerización brinda muchos beneficios a las compañías. Por ejemplo, tener acceso a capacidades y experticia de manera más rápida** y que quizás no tengan internamente. Es de entender que la tecnología avanza a gran velocidad, haciendo que los equipos de trabajo de seguridad necesiten estar actualizándose, conociendo nuevas soluciones, herramientas, técnicas y estándares. **Las compañías dedicadas a entregar estos servicios se capacitan y actualizan continuamente sobre las novedades que emergen;** en cambio, los equipos de trabajo internos estarán enfocados en atender las situaciones propias de su área.

4

Entrevistador

¿Qué factores debe tener en cuenta una empresa para tomar esta decisión de tercerización y cuáles son las ventajas que pueden salir de esto?

Experto Axity

Ahora bien, tomar la decisión de **tercerizar implica identificar y asegurarse que el outsourcing cuente con la experiencia suficiente,** demostrando que la empresa a contratar ya ha desarrollado capacidades en el servicio que va a prestar. Pero no solo eso, **también debe tener políticas, procesos y procedimientos establecidos y madurados para la ejecución de las tareas** e, igualmente, deben estar alineados a las buenas prácticas de la industria y acorde a los estándares de seguridad existentes. Finalmente, los estudios y certificaciones que hayan obtenido, tanto el outsourcing como su personal, dará una mayor garantía de que conoce la industria, el servicio y/o las actividades que se van a ejecutar durante la prestación del servicio.

¡Conoce más sobre nuestras soluciones de ciberseguridad aquí!

4

Una vez tomada esta decisión,

Entrevistador

¿cómo definir una estrategia junto a los proveedores expertos de soluciones tecnológicas que cubra en su totalidad las necesidades de cada organización?

Experto Axity

Definir una estrategia implica un trabajo conjunto entre la organización y el proveedor de seguridad. En este caso, en Axity entraríamos a jugar un papel determinante. Gracias a toda la experiencia, los procesos, las alianzas y la madurez que hemos desarrollado en temas de seguridad, serviremos de apoyo a las organizaciones, tanto en la implementación de los controles adecuados de seguridad como en desarrollar madurez y automatización en cada una de las tareas que se deben ejecutar.

Además, al ser un trabajo conjunto, las organizaciones (dependiendo de su grado de madurez) deben saber a dónde quieren llegar.

Con este trabajo en equipo, apoyaremos no solo en la implementación de los controles, sino desde el momento en que se defina la estrategia. Esto, con el fin de identificar con exactitud qué requerimientos tiene el negocio, así como las tecnologías que se deberían usar, siempre buscando que el cliente obtenga el mejor costo beneficio.

volver al índice

5 El activo principal: la información

La información es considerada hoy uno de los activos más relevantes para las organizaciones a nivel mundial. En el contexto de ciberamenazas actual.

Entrevistador

¿Con cuáles tipos de tecnologías destinadas a la protección de la información y de sus sistemas contra amenazas debe contar cada entidad?

¿Cuál es el alcance de las capacidades de estas tecnologías de detección y protección?

Experto Axity

Actualmente hay una gran variedad de tecnologías y soluciones, así como de fabricantes de esas tecnologías. Cada una tiene un enfoque concreto o proporciona protección de acuerdo con su especialidad; la definición de los controles y las herramientas tecnológicas que se deberían tener dependerá mucho del resultado del análisis de riesgo que se realice.

En las definiciones de seguridad existen tecnologías estándar que toda arquitectura de seguridad debería tener: las tecnologías para la protección perimetral, la protección de los recursos en nube, la protección del endpoint, la protección de las aplicaciones, la protección del desarrollo. En general, **en todo punto o lugar donde haya o transite información se necesita implementar protección a través un control tecnológico.** Adicional a esta, también debe haber visibilidad del tráfico, de los eventos e incidentes de seguridad y de las amenazas que pueda tener la información y el negocio.

5

Entrevistador

¿Con cuáles tipos de tecnologías destinadas a la protección de la información y de sus sistemas contra amenazas debe contar cada entidad?

¿Cuál es el alcance de las capacidades de estas tecnologías de detección y protección?

Experto Axity

Axity apoya a las organizaciones en la identificación y definición de las tecnologías que sean acordes al negocio y que protejan la información de nuestros clientes, y cuenta con diferentes alianzas de fabricantes tecnológicos para proveer los controles de seguridad end to end, es decir en todos los puntos donde se requiere protección.

Hoy en día existe un enfoque que ayuda a las organizaciones en la definición de los controles tecnológicos. Se trata del **modelo Zero Trust o Cero Confianza,** y tiene por objetivo que las organizaciones no confíen en nada de manera predeterminada, independientemente de donde provenga, y que solo permita lo exclusivamente necesario para operar.

Basado en este modelo, **Axity ofrece la tecnología necesaria y adecuada para la protección y seguridad de la información sin importar donde se encuentre ubicada y desde el lugar que se acceda.**

¿Conoces el modelo Zero Trust?

Zero Trust implica SIEMPRE desconfiar de usuarios y dispositivos, mínimos privilegios, automatización, ciberinteligencia y Machine Learning. En este modelo el usuario solo conseguirá acceso a aquellos recursos para los que contará con autorización y siempre después de haber sido correctamente identificado.

Se debe aplicar en los inicios de sesión, la autenticación passwordless, cada usuario solo debe disponer de los permisos que sean realmente necesarios. Algunas de las herramientas son: EDR (Endpoint Detection and Response), Cloud Access Security Broker (CASB); toda organización debe contar con una red definida por software (SDN); cada SOC debe disponer de un SOAR (Security Orchestration, Automation and Response) de última generación.

volver al índice

6 Ataques de negación de servicio (DDoS) en auge

Existe un auge en el cibercrimen respecto al uso de ataques de negación de servicio para afectar las operaciones de las empresas y ocasionar impactos negativos en sus resultados.

Entrevistador

¿Qué tipo de optimización y actualización de herramientas para la protección de DDoS se debe implementar en las organizaciones para reducir los riesgos de estos ataques?

Experto Axity

El DDoS es un tipo de ataque que busca detener las operaciones de las organizaciones. Las plataformas de TI cuentan con un límite de capacidad y al ser superadas por las peticiones o transacciones que los atacantes envían, colapsan y dejan de funcionar temporalmente, causando el ataque. **Para esto existen tecnologías especializadas que permiten identificar los ataques,** bloqueando ese tráfico inusual y permitiendo el tráfico que de acuerdo con sus métodos de aprendizaje considera limpio y correcto.

volver al índice

7

Inteligencia ante las amenazas: monitoreo 24/7

Para finalizar, hablemos sobre la inteligencia ante las amenazas con la que deben contar las organizaciones. El constante cambio y evolución tecnológica demanda que los modelos de operaciones que usemos sean 24/7 y que cuente con información actualizada sobre las situaciones de amenazas y riesgos.

Entrevistador

¿Cómo se realiza este proceso de recolección, almacenamiento, divulgación y concientización de esta información?

¿Cómo generar un análisis de inteligencia de amenazas y procesos de preparación y respuesta óptimos?

Experto Axity

La inteligencia de amenazas, como su nombre lo indica, busca aplicar análisis a las amenazas que se presentan o se pueden presentar. Hoy en día, **al contar con un proceso de inteligencia las organizaciones pueden identificar de manera proactiva las amenazas que pueden afectar a la información y al negocio, con el fin de actuar de manera temprana y evitando posibles daños o pérdidas.**

Los conceptos de inteligencia de amenazas y caza de amenazas se refieren a contar con personal experto y tecnología adecuada para identificar, tanto en el entorno interno como externo de la organización, cualquier aspecto que podría llegar a afectar.

Estos aspectos son indicadores de compromiso, con los que los especialistas de threat intelligence hacen análisis y correlación de lo que ocurre y definen las acciones pertinentes para evitar que una amenaza se haga efectiva.

7

Entrevistador

¿Cómo se realiza este proceso de recolección, almacenamiento, divulgación y concientización de esta información?

¿Cómo generar un análisis de inteligencia de amenazas y procesos de preparación y respuesta óptimos?

Experto Axity

Este monitoreo, identificación y análisis debe realizarse continuamente, en modalidad 24/7, puesto que los atacantes están continuamente buscando maneras de generar nuevos ataques.

Axity cuenta con un servicio de SOC desde el cual monitorea continuamente e identifica estas amenazas, brindando visibilidad de lo que está ocurriendo y de lo que pueda afectar la información, la infraestructura o el negocio de nuestros clientes.

¡Descubre más de SOC en este enlace!

volver al índice

Nuestro gerente de Ciberseguridad, **Hensy Hernández,** al igual que nuestro equipo Axity, reitera la importancia de conocer los **objetivos particulares de la empresa y sus necesidades,** así como el estado de madurez de ciberseguridad. Sobre todo, saber contar con aliados estratégicos que cuenten con la experiencia y el conocimiento para acompañar y apoyar el proceso de fortalecimiento de ciberseguridad, desde su planeación hasta la implementación.

Explora nuestro portal TI

https://www.axity.com/es/blog-comunidad-axity/

Contáctanos

contacto@axity.com

Sé parte de nuestra comunidad

 *axity.social*

 *axity_social*

 *axity_social*