GRUPO ÁGUILAS
Seguridad Privada

ÁGUILAS NEWS

Edición Marzo

www.grupoaguilas.com

IMPORTANCIA DEL ANÁLISIS DE DATOS EN LA TOMA DE DECISIONES

Pero, ¿por qué es importante el análisis de datos en la toma de decisiones? Las experiencias con este proceso evidencian que las empresas, en promedio, generan mayores ingresos y acceden a nuevas oportunidades comerciales. Es más, según IDG, el 64 % de los responsables de la toma de decisiones de TI señala que la recopilación y el análisis de datos ha cambiado la forma de hacer negocios durante los últimos tres años.

Entre los principales beneficios que brinda esta práctica, podemos mencionar a los siguientes:

MEJORA EL ANÁLISIS DE LAS ALTERNATIVAS

El análisis de datos, con objetivos empresariales claros, realizado de manera correcta y utilizando "buenos" datos, permite analizar mejor las alternativas, abre un nuevo abanico de posibilidades y mejora el conocimiento que se tiene de cada una de ellas. Esto último aumenta la probabilidad de que la elección de la mejor alternativa lleve a un resultado exitoso.

REDUCE COSTOS

Implementar el análisis de datos en la toma de decisiones ayuda a identificar posibles tácticas que reduzcan los costos en las diferentes áreas del negocio. De acuerdo a Bi-Survey, **las empresas que utilizan el análisis de Big Data disminuyen sus costos en un 10 %.** Pero, ¿qué hace ello posible? Esta práctica permite detectar estrategias que están siendo ineficaces, pero que aun así se les está asignando gran parte del presupuesto.

REDUCE RIESGOS

La toma de decisiones al azar puede desencadenar graves pérdidas económicas para la organización. Por el contrario, tomar decisiones basadas en datos duros, facilita el análisis costo-beneficio y manejo de escenarios, lo que disminuye las posibilidades de cometer errores al considerar las consecuencias posibles, lo cual es útil cuando se realizan grandes inversiones o apuestas en proyectos de alto riesgo.

ÁGUILAS CORP.

ÁGIL Y RÁPIDA ADAPTABILIDAD

El análisis de datos permite predecir tendencias futuras del mercado y responder rápidamente a ellas, ofreciéndole la posibilidad de una mejor ventaja competitiva a la empresa en su mercado objetivo. Para esto, es necesario que la compañía tenga la capacidad organizacional de la "agilidad". El análisis de datos brinda el conocimiento, pero si la organización no puede responder a ello, su adaptación no va a ocurrir.

PANOPTIC
Monitoreo Inteligente

Con nuestra plataforma **PANOPTIC** podrás gestionar en tu organización la seguridad patrimonial e higiene y salud a través del módulo de **Predictive Analytics.**

Predictive Analytics te ofrece eliminar el trabajo manual así como un análisis de todos los datos de las actividades que requiere tu operación, este análisis avanzado te permite visualizar tus los resultados de tu operación, para predecir las acciones a seguir.

Data predictive te permite obtener información para una mejor administración de tu recurso humano mostrándote indicadores de:

- Cobertura
- Asistencias
- Bajas
- Incapacidades
- Vacantes
- Rotación
- Faltas
- Capacitación

https://www.esan.edu.pe/conexion-esan/importancia-del-analisis-de-datos-en-la-toma-de-decisiones

EL PODCAST

GRUPO ÁGUILAS

Te invitamos a escuchar nuestro podcast en donde hablamos de temas relevantes dentro de la seguridad.

Spotify

Encuéntranos como:

El Podcast de Grupo Águilas

ÁGUILAS CORP.

SIGUE

Seguimiento interno a guardias y empleados

AHORA PODEMOS AYUDARTE MÁS RÁPIDO Y FÁCIL

Podemos atender dudas sobre tu **nómina**, **vacaciones**, **DT**, **supervisión**, **uniformes**, etc.

HORARIO DE ATENCIÓN

Lunes a Viernes

7:00 am a 5:00 pm

(656) 398 - 0777

(656) 418 - 3365

sigue@grupoaguilas.com

ÁGUILAS CORP.

EN 2022, 13.2% MÁS MUJERES VÍCTIMAS DE LA VIOLENCIA ♀

La violencia contra la mujer en México no cesa. Cada día, 340 son víctimas del delito, revelan las más recientes cifras del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP).

Los datos muestran que, **en 2022, hay un incremento de 13.2% en el número de mujeres víctimas del delito, con relación a 2021, y 9.9% de alza en el número de denuncias que mujeres presentan ante el Ministerio Público.**

En la primera se indica que ilícitos como homicidio doloso y culposo, lesiones dolosas y culposas o extorsión registran durante 2022 un incremento en el número de mujeres víctimas, con relación a 2021.

Mientras que, **en el caso de denuncias, hay alza en delitos como incesto, acoso sexual, hostigamiento sexual, violencia de género, violación equiparada, abuso sexual, aborto, violencia familiar y violación simple.**

Entre los pocos delitos que en ambas estadísticas registran en 2022 una disminución, con relación a 2021, está el feminicidio, el cual tiene una baja de 8% en el número de víctimas y 6.8 por ciento en denuncias.

Según las cifras del SESNSP, la violencia familiar es el delito más denunciado por las mujeres en México. En el periodo enero-octubre de 2022 hubo 230 mil 30 denuncias, 7% más que en el mismo lapso de 2021.

Feminicidios
-8%

Violencia familair
+7%

Los delitos de mayor incremento de denuncias en el periodo enero-octubre de 2022, con relación al mismo lapso de 2021, son:

Incesto
+120%

Acoso sexual
+55%

Hsotigamiento sexual
+32%

Violación equparada
+30%

ÁGUILAS CORP.

En tanto, los delitos con mayor incremento en el número de víctimas son:

Trata de personas
+25.2%

Lesiones culposas
+25%

Corrupción de menores
+22.3%

Homicidio culposo
+16.6%

Extorsión
+15.1%

En Grupo Águilas queremos que que te sientas segura en todo momento por lo que con neuestro botón de pánico contaras con la ayuda de nuestros expertos que te podran auxiliar en caso de una emergencia.

Nuestro BOTÓN DE PÁNICO te permite:

Recibir información sobre los lugares seguros más cercanos como hospitales, estaciones de policía etc.

Recibir notificaciones de tráfico, clima ó accidentes en carretera.

Recibir apoyo de nuestra central de monitoreo en caso de una emergencia.

Estar monitoreado por un equipo de especialistas en seguridad. Llamar a un contacto de emergencia.

https://www.elfinanciero.com.mx/nacional/2022/11/24/en-2022-132-mas-mujeres-victimas-de-la-violencia/

3 TENDENCIAS EN CIBERSEGURIDAD QUE COBRARÁN ESPECIAL IMPORTANCIA EN 2023

Para la mayoría de las empresas el año 2022 fue muy turbulento. Entre la inflación y la crisis energética, la seguridad informática ha coqueteado con caer en el olvido. Sin embargo, eso sería un grave error, puesto que, la ciberseguridad debe abordarse de forma proactiva este año.

1 Asegurar las cadenas de suministro: físicas y digitales

Además de las cadenas de suministro físico de productos, esto también se aplica a la cadena de suministro de software.

En las cadenas de suministro de hardware, por ejemplo, es importante comprobar si los componentes conectados en red son originales. Mientras tanto, circulan por aquí grandes cantidades de mercancías falsificadas que no se pueden distinguir fácilmente de las auténticas. El firmware inseguro de estos componentes puede convertirse en una peligrosa puerta de entrada a los sistemas conectados en red.

En el ámbito del software, se pueden utilizar las llamadas listas de materiales de software (SBOM), que muestran qué componentes (de código abierto) se han utilizado. Además, las relaciones entre los distintos componentes de la cadena de suministro de software se hacen transparentes. Esto permite identificar más rápidamente el origen de las vulnerabilidades en el software. Recientemente se ha exigido a las autoridades estadounidenses que soliciten un SBOM y la documentación del proceso a sus proveedores de software para garantizar la integridad del código.

2 Informática confidencial

La nube es ineludible y cada vez son más las cargas de trabajo críticas que se trasladan allí. Sin embargo, esto también aumenta la necesidad de seguridad. Además, las empresas deben asegurarse de que no entren en conflicto con el GDPR europeo a través de sus relaciones comerciales con los grandes hiperescaladores estadounidenses. También existen requisitos de cumplimiento específicos de la industria.

En este contexto, la informática confidencial describe un enfoque para blindar el procesamiento de datos en la nube de tal forma que ni siquiera el proveedor tenga conocimiento de ello. Los datos permanecen encriptados el mayor tiempo posible y durante la ejecución se encuentran en un exclave cerrado, es decir, una máquina virtual o un contenedor. Esto, a su vez, crea la necesidad de gestionar las identidades de los usuarios para autorizar su acceso. Los proveedores criptográficos pueden ayudar con esto y con la gestión de claves para el cifrado de datos. En el futuro, cada vez más empresas confiarán en el cifrado en la nube y, por tanto, también aumentará la demanda de criptografía, gestión de claves y raíz de confianza de hardware.

3 Gestión de criptoactivos

A menudo, las empresas actuales ni siquiera son conscientes del tipo de criptografía que utilizan realmente, de los certificados que emplean ni de cuándo caducan. Existe una gran incertidumbre y la necesidad de conocer mejor la propia infraestructura y de asegurar los distintos canales de comunicación es cada vez mayor. Por esta razón, las empresas preocupadas por la seguridad están iniciando cada vez más evaluaciones de criptografía. Otro paso es la gestión de activos con visión de futuro, por ejemplo, cuando un algoritmo está obsoleto. En el futuro, será importante encontrar soluciones y definir procesos para modernizar continuamente sus propios activos criptográficos. El objetivo es lograr la llamada criptoagilidad, de forma que los algoritmos se adapten directamente si se rompe un determinado método de encriptación, por ejemplo, mediante ordenadores cuánticos.

GROOMING

QUÉ ES, CÓMO DETECTARLO Y PREVENIRLO

El grooming y, en su evolución digital, el online grooming (acoso y abuso sexual online) son formas delictivas de acoso que implican a un adulto que se pone en contacto con un niño, niña o adolescente con el fin de ganarse poco a poco su confianza para luego involucrarle en una actividad sexual.

Esta práctica tiene diferentes niveles de interacción y peligro: desde hablar de sexo y conseguir material íntimo, hasta llegar a mantener un encuentro sexual.

Se trata de un proceso en el que se produce un vínculo de confianza entre la víctima y el acosador. Este intenta aislar poco a poco al menor, y lo consigue desprendiéndolo de su red de apoyo (familiares, profesores, amigos, etc.) y generando un ambiente de secretismo e intimidad.

LAS FASES DEL 'ONLINE GROOMING'

El online grooming incluye una serie de conductas que pueden ser desordenadas, pero, por lo general, existen patrones de conducta y fases comunes que vamos a ver a continuación para poder detectarlo y prevenirlo.

La creación de un vínculo de confianza. En muchos casos a través de sobornos o engaños el agresor contacta con la niña o niño y establece el vínculo de confianza. Para ello normalmente finge otra edad, muy cercana a la de la víctima. Además, puede que el abusador haga regalos, empatice a un nivel profundo con los niños y niñas haciendo que escucha sus problemas y aproveche esa información para chantajear después.

El aislamiento de la víctima. En esta fase el agresor persigue arrancar la red de apoyo natural del menor (familiares, amistades, docentes, etc.) dejándolo desprotegido. De esta manera insiste en la necesidad de mantener todo en secreto.

La valoración de los riesgos. El agresor tiende siempre a asegurar su posición, así que suele preguntar a la víctima si alguien más conoce su relación e intenta averiguar quién más tiene acceso al ordenador o dispositivo que utiliza el menor.

Conversaciones sobre sexo. Una vez se siente con confianza, el abusador empieza a introducir conversaciones sexuales de manera paulatina. Busca que la víctima se familiarice tanto con la temática sexual como con el vocabulario.

Las peticiones de naturaleza sexual. Este es el objetivo principal del online grooming. En esta última fase el criminal utiliza la manipulación, las amenazas, el chantaje o la coerción para que la víctima le envíe material sexual, relate fantasías sexuales o la relación culmine con un encuentro físico.

¿CÓMO PREVENIR EL 'GROOMING'?

Ante un fenómeno tan complejo, la respuesta debe ser integral y la forma más eficaz de actuar contra la violencia viral se basa en la prevención. Lo más indicado es intervenir en la educación en positivo a niños, niñas y adolescentes.

En primer lugar, es necesaria una educación afectivo-sexual, que forme a los más jóvenes en materia de sexualidad, y al mismo tiempo es importante la formación en un uso seguro y responsable de las herramientas digitales.

Es esencial tener en cuenta que especialmente en el online grooming el engaño es lento y no hay consentimiento del niño o niña, no son conscientes de lo que les ocurre, y no tienen las herramientas adecuadas para defenderse. **Nunca podrá ser culpa de ellos.**

En definitiva, **la comunicación y la educación afectivo-sexual, juntas con el apoyo del entorno más cercano a los menores, son las herramientas más eficaces,** tanto para prevenir la violencia, así como para no perpetuar sus consecuencias a largo plazo.

ÁGUILAS CORP.

NUESTRAS REDES SOCIALES

Encuéntranos como:

Grupo Águilas Seguridad Privada

GRUPO ÁGUILAS
Seguridad Privada

Encuéntranos como
Grupo Águilas Seguridad Privada

ÁGUILAS CORP.

www.grupoaguilas.com