MINSAIT BRINDA RECOMENDACIONES DE CIBERSEGURIDAD PARA PROTEGER LA INFORMACIÓN CORE DE LAS EMPRESAS EN 2020

- **La compañía de Indra recomienda la implementación de un programa de Gestión de Riesgo Digital que permita controlar la seguridad, desde la prevención a la predicción y la respuesta ante la amenaza**

- **Los objetivos de ciberseguridad de las compañías en general deben estar alineados a la estrategia de negocio, protegiendo principalmente la información de la actividad principal que desarrolle la empresa como tal**

- **Indra, que recientemente ha adquirido la compañía de ciberseguridad SIA para reforzar su liderazgo en este ámbito, tiene un equipo de más de 1.000 especialistas, una oferta de valor diferencial y completa, y tres centros avanzados de ciberseguridad, dos en Latinoamérica**

Lima, 13 de enero de 2020.- Los cibercriminales atacan a las empresas de forma repetitiva y constante, porque saben que un solo ataque exitoso les permitirá obtener información que podrá traducirse en mucho dinero. Frente a esta situación, Minsait, una compañía de Indra, recomienda la implementación de un programa de Gestión de Riesgo Digital que controle la seguridad, desde la prevención a la predicción y la respuesta.

Carlos Fernández, responsable Global de Venta especializada de Ciberseguridad de Minsait, empresa líder en consultoría de transformación digital y Tecnologías de la Información en España y Latinoamérica, brinda las siguientes recomendaciones que, desde la compañía, plantean en materia de ciberseguridad, a fin de que las empresas puedan afrontar exitosamente los principales retos que, en esta materia, puedan plantearse en un futuro. Para el experto, es importante:

- **Alinear los objetivos de ciberseguridad con las iniciativas, estrategias y prioridades de negocio:** el Plan de Gestión de Riesgo Digital debe centrarse, sobre todo, en la protección de la información de la actividad principal del negocio (core business), dado que de ella depende su subsistencia y crecimiento. Esta información incluye contratos, planes estratégicos, objetivos, proyecciones, facturas, correos de coordinación entre gerencias, o bases de datos, entre otros.

- **Evaluar el riesgo digital y no solo de las plataformas tecnológicas:** cada empresa es responsable de saber cuál es su información más sensible y los procesos que la hacen vulnerable frente a un ataque. No basta la instalación de antivirus en los equipos, sino que también es necesaria la identificación de posibles riesgos en la manipulación de la data y conocer cómo los cibercriminales podrían intentar acceder a ella.

- **Establecer mecanismos avanzados de detección y respuesta:** el plan de respuesta y gestión de incidentes de seguridad se desarrollará de acuerdo con el tipo de ataque y al atacante. La táctica de respuesta no puede ser la misma cuando el ataque ha sido realizado por realizado un grupo cibercriminal, hacktivista o geopolítico, que cuando se trata de una campaña global de phishing para ver quien “cae” en la trampa.

  Así como hay ataques que se materializan de forma inmediata, hay otros que se alojan en los sistemas para quedarse durante días o meses. “Para dimensionar el impacto tomemos un ataque de extorsión digital por Ransomware, por ejemplo. Puede afectar a la disponibilidad de los servicios al cifrar todos los archivos de un sistema o una red, además de un daño reputacional, y aún más si no tiene respaldos”, detalla el experto de Minsait quien añade que, precisamente por ello, además de

Comunicación y Relaciones con los Medios
ATREVIA
Sonia Ramos
940171717
sramos@atrevia.com

contar con la tradicional protección en ciberseguridad, es importante añadir componentes de detección avanzados (tecnologías de UEBA - User and Entity Behaviour Analytics - como la solución de Minsait de última generación Onesait Behaviour Fraud, para la detección de fraude en operaciones de pago y transferencias online que multiplica los niveles de protección gracias a la aplicación de técnicas pioneras de inteligencia artificial que son capaces de replicar los procedimientos y la forma de trabajar de los analistas bancarios especializados.).

Otras recomendaciones generales de seguridad informática para empresas son contar con mecanismos de reporte de sospechas por parte de los usuarios; restringir el acceso a redes sociales, emails no corporativos y páginas web dudosas; limitar el uso de dispositivos USB y establecer mecanismos de contraseñas robustas (doble factor de autentificación).

Identificación temprana de riesgos de seguridad

Una adecuada capacitación a los colaboradores sobre el protocolo de ciberseguridad y alerta temprana de su compañía, puede hacer que esta sea más resistente frente a los ataques. Para lograr este objetivo, se debe establecer un programa completo que incluya:

- **Formación genérica respecto a los riesgos de ataque más comunes**: entre estos se encuentran el phishing (adjuntos con Malware o URLs maliciosas), la ingeniería social (mensajes engañosos), la navegación web en páginas dudosas y la conexión a dispositivos extraíbles USB.

  Asimismo, los colaboradores deben ser concientizados para que siempre verifiquen la validez de los certificados de seguridad de las webs en barra del navegador (browser), repasen con cuidado los remitentes y direcciones de correo electrónico, reporten al departamento de seguridad o sistemas cualquier email sospechoso (sin abrir adjuntos ni hacer click en enlaces) y para que no publiquen información sobre su trabajo en redes sociales.

- **Formación al Top Management**: los ejecutivos con poder de toma de decisiones dentro de las empresas y organizaciones, son uno de los principales blancos para los ciberdelincuentes, dado su acceso a la información más sensible de sus organizaciones. Estos ataques dirigidos específicamente a gerentes y ejecutivos de alto rango se conoce como “whaling” y usualmente hace uso de tácticas de ingeniería social para obtener información clasificada.

  Además, existe el riesgo permanente de una suplantación de identidad, mediante la cual el criminal puede utilizar la firma digital o correo del ejecutivo para estafar a otras personas, causando daño económico y reputacional a la compañía.

- **Capacitación de los departamentos en función de riesgos específicos:** luego de identificar las posibles amenazas en cada área (administración, sistemas, recursos humanos, finanzas, gerencia general, entre otras) se procederá a aplicar precauciones específicas, dependiendo de la forma cómo se maneja la información en cada una de ellas.Si bien hay un cuerpo de mejores prácticas que aplican a todos los departamentos desde el programa de Gestión de Riesgos, se deben determinar los controles ya que no es ni efectivo ni eficiente poner los mismos protocolos de seguridad en todas.

Liderazgo en servicios de ciberseguridad

Indra es la empresa líder en el mercado de la seguridad de la información en España y Portugal, y una de las compañías de referencia en Latinoamérica en materia de ciberseguridad. Precisamente, para reforzar su actividad en este ámbito, Indra ha adquirido recientemente SIA, una compañía especializada en servicios de ciberseguridad.

Con esta integración, Indra incrementa su oferta, la hace más integrada y aumenta su presencia global para dar respuesta a amenazas globales. La unidad de Ciberseguridad de Indra está formada por un equipo de más de 1.000 profesionales altamente cualificados y expertos en este ámbito, conformados en equipos especializados de consultoría en diferentes áreas, muy complementarios.

Comunicación y Relaciones con los Medios
ATREVIA
Sonia Ramos
940171717
sramos@atrevia.com

En Latinoamérica, Indra ha implantado dos de sus tres centros avanzados de ciberseguridad, uno en Ciudad de México y otro en Bogotá (Colombia), desde los que presta servicios de protección y seguridad de forma integral.

Acerca de Minsait

Minsait, una compañía de Indra (www.minsait.com), es una empresa líder en consultoría de transformación digital y Tecnologías de la Información en España y Latinoamérica. Minsait presenta un alto grado de especialización y conocimiento sectorial, que complementa con su alta capacidad para integrar el mundo core con el mundo digital, su liderazgo en innovación y en transformación digital y su flexibilidad. Con ello, enfoca su oferta en propuestas de valor de alto impacto, basadas en soluciones end-to-end, con una notable segmentación, lo que le permite alcanzar impactos tangibles para sus clientes en cada industria bajo un enfoque transformacional. Sus capacidades y su liderazgo se muestran en su oferta de productos, bajo la denominación Onesait, y su oferta transversal de servicios.

Indra en Perú

Presente en Perú desde 1987, Indra es en una de las compañías más importantes de tecnología y consultoría del país, contando con más de 1.500 profesionales. Actualmente forma parte de algunos de los proyectos innovadores clave para el desarrollo económico y tecnológico en los sectores de Transporte & Defensa, y de Tecnologías de la Información (TI) a través de su filial Minsait.

Acerca de Indra

Indra (www.indracompany.com) es una de las principales compañías globales de tecnología y consultoría y el socio tecnológico para las operaciones clave de los negocios de sus clientes en todo el mundo. Es un proveedor líder mundial de soluciones propias en segmentos específicos de los mercados de Transporte y Defensa, y una empresa líder en consultoría de transformación digital y Tecnologías de la Información en España y Latinoamérica a través de su filial Minsait. Su modelo de negocio está basado en una oferta integral de productos propios, con un enfoque end-to-end, de alto valor y con un elevado componente de innovación. En el ejercicio 2018, Indra tuvo unos ingresos de 3.104 millones de euros, 43.000 empleados, presencia local en 46 países y operaciones comerciales en más de 140 países.

Comunicación y Relaciones con los Medios
ATREVIA
Sonia Ramos
940171717
sramos@atrevia.com