

Gipuzkoa pondrá en marcha ZIUR, su centro de ciberseguridad en el segundo semestre del año

Según lo previsto, Euskadi contará desde el próximo otoño con un segundo centro de ciberseguridad. Bajo la denominación de **ZIUR Centro de Ciberseguridad Industrial de Gipuzkoa**, cuenta con una financiación de 1,5 millones de euros que aportará la institución foral para su primer año de funcionamiento. Esta noticia fue anunciada por la diputada de Promoción Económica, **Ainhoa Aizpuru**, en el acto de presentación del evento vasco IndustrySec, celebrado los pasados 10 y 11 de mayo, y corroborado durante el acto inaugural del mismo por **Markel Olano**, diputado general de Gipuzkoa, quien ha apostado por explotar la gran capacidad ofrecida por Gipuzkoa en el ámbito de la ciberseguridad. "Contamos con un potencial enorme para seguir generando nuevo tejido económico, contamos con empresas punteras, con un conocimiento amplio, contrastado e innovador", ha subrayado.

En este contexto, reveló que ZIUR, que se sitúa en el marco de Etorikizu-



na Eraikiz y abrirá sus puertas en el segundo semestre de este año, parte con la vocación de ser columna central e impulsar el nivel de especialización del territorio en este nicho y, al mismo tiempo, blindar la seguridad de un sector industrial que es seña de identidad del tejido productivo guipuzcoano.

Como es sabido la irrupción de Ziur supondrá la coexistencia con el denominado **Centro Vasco de Ciberseguridad** auspiciado por el Gobierno vasco y SPRI, con sede en Vitoria y puesto en marcha en octubre de 2017. Es pretensión que tenga la capacidad para inves-



Edificio Urola, en el PT. de Zuzatu, que albergará ZIUR
Fotografía: Michelena

tigar y probar productos y servicios de las empresas vascas, así como emitir certificaciones que acrediten que son ciberseguras. Aizpuru confirmó que la adecuación de las instalaciones que acogerán el centro "ya ha concluido su primera fase".

En concreto, el centro se ubicará en el parque empresarial Zuzatu de San Sebastián. Dispondrá de un local de 250 metros cuadrados en los que se instalará un espacio para la formación,

otro para emprendedoras y un laboratorio, y contará con siete personas en su plantilla, un director, un responsable técnico que trabajará junto a tres empleados, un administrativo y un encargado de las labores de comunicación y comerciales.

Markel Olano, Alcalde de San Sebastián, explicó que un estudio realizado por la institución foral este verano constató que el 84% de las empresas guipuzcoanas afirma contar con equipos de producción conectados a redes corporativas o públicas, que una de cada tres señala que no tiene protocolos adecuados de ciberprotección y que el 53% ha reconocido haber sufrido un ciberataque recientemente. Con estos datos, se ha justificado la necesidad de poner en marcha un centro en Gipuzkoa poco después del que ha implantado el Gobierno Vasco en Álava para toda la Comunidad Autónoma y que también atenderá al sector industrial.

INNOTEC participa en La Voz de la Industria y pone en marcha el blog Hacks&Labs

InnoTec fue participante del primer encuentro de 'La Voz de la Industria', celebrado el pasado 24 de mayo en México de la mano del **Centro de Ciberseguridad Industrial (CCI)**. Durante el encuentro, se presentaron los resultados preliminares del estudio sobre el estado de la ciberseguridad



Entelgy

en marcha un nuevo sitio web -www.hacksandlabs.com- que albergará artículos técnicos fruto de la investigación y trabajo de sus profesionales en materia de ciberseguridad.



El mundo *hacking*, la respuesta y gestión de incidentes, los sistemas de control industrial o la gestión de vulnerabilidades, entre otros campos, son los principales temas que se abordarán en el *blog*. Para empezar, la página web ya cuenta con una serie de interesantes artículos como 'Adversarial examples para reconocimiento facial', 'Write Up Hacker One H1-212' sobre la resolución de un reto de seguridad o CTF y 'Explotación de Weblogic CVE-2017-10271 en entornos basados', entre otros.

El mundo *hacking*, la respuesta y gestión de incidentes, los sistemas de control industrial o la gestión de vulnerabilidades, entre otros campos, son los principales temas que se abordarán en el *blog*. Para empezar, la página web ya cuenta con una serie de interesantes artículos como 'Adversarial examples para reconocimiento facial', 'Write Up Hacker One H1-212' sobre la resolución de un reto de seguridad o CTF y 'Explotación de Weblogic CVE-2017-10271 en entornos basados', entre otros.

FORTINET se une a los servicios X-Force de IBM y firma un acuerdo con ARISTA NETWORKS

Fortinet se ha unido a los nuevos Servicios de Gestión de Amenazas X-Force de IBM. Este acuerdo permitirá a ambas organizaciones proporcionar a sus clientes una visibilidad de las amenazas desconocidas hasta ahora, detección y prevención de ataques, así como una estrategia integrada de defensa en profundidad diseñada para abarcar toda la superficie de ataque de una organización.

Cabe recordar que IBM Security forma parte del programa Fabric-Ready de Fortinet desde 2017, aunando la protección de seguridad integral de Fortinet con la seguridad empresarial de IBM al objeto de ofrecer una protección avanzada además de soporte frente a ciberamenazas sofisticadas, tanto en entornos de red como multi-nube.

Arista se une al programa Fabric-Ready de Fortinet.

De forma paralela, la compañía Arista Networks, proveedor de soluciones de red en la nube definidas por software para grandes centros de datos, y entor-

nos de almacenamiento y alto rendimiento, se ha unido al programa de socios Fabric-Ready de Fortinet.

Se trata de un paso más en la colaboración entre Fortinet y Arista y su compromiso de aumentar la seguridad de los centros de datos dinámicos y las redes en la nube. En este sentido, al aprovechar la capacidad de programación del EOS de Arista con Fortinet Security Fabric, Arista DirectFlow Assist ofrecerá una arquitectura de escalabilidad donde el *switch* pueda descargar el tráfico del cofuegos, permitiendo a los administradores de red dimensionar *firewall* según los patrones de tráfico normales, lo que reduce en una mayor escalabilidad y ahorro de costes.

Al mismo tiempo, al combinar Fortinet Security Fabric con la extensibilidad de las soluciones de red en la nube de Arista, incluidos los Servicios de Macro Segmentación Arista CloudVision (MS), los centros de datos tendrán la oportunidad de cubrir sus necesidades de seguridad con mayor flexibilidad, control y automatización.

FORTINET.

