CATÁLOGO SOCIOS

CIBERSEGURIDAD

aertic Agrupación Empresarial Innovadora del sector TIC de La Rioja

fer federación de empresas de la rioja

CIBERSEGURIDAD

POR UNA DIGITALIZACIÓN SEGURA

El avance de la digitalización y el despliegue de todas sus potencialidades de desarrollo y crecimiento para las personas y las empresas, entraña riesgos, como la protección de privacidad digital para evitar el acceso no autorizado a los datos, que hay que evitar.

Consciente de ello, la Agrupación Empresarial Innovadora del sector TIC (AERTIC) ha reunido en este documento a sus empresas socias especializadas en la oferta de servicios de ciberseguridad, y los ha desgranado para que las empresas de todos los sectores conozcan qué soluciones existen y puedan llevarlas a cabo con su ayuda. Asimismo, y con el fin de explicar en qué consisten muchos de los términos empleados para denominar las herramientas y soluciones se ha incluido un glosario que pretende despejar estas dudas.

La creciente conectividad entre equipos (IoT) y el crecimiento del ciberespacio como ámbito para los intercambios comerciales o almacenamiento de datos hacen que la ciberseguridad se deba convertir en una prioridad.

Del mismo modo que en el mundo físico nadie duda de la necesidad de implementar medidas de seguridad para proteger la integridad de las instalaciones o del patrimonio de personas y entidades (sistemas de video vigilancia, contratación de alarma, existencia de un sistema de control de accesos, etc) en nuestros sistemas informáticos y en el ciberespacio quedan depositados importantes activos (datos, clientes, protocolos, formularios, bases de datos, contactos, claves de acceso, sistemas de intercambio, tiendas virtuales…) que precisan de protección.

Preservar la integridad y confidencialidad de las comunicaciones y de los datos adquiere una importancia capital e imprescindible dentro de las empresas, dado el valor tangible e intangible que entraña y que afecta, en muchos casos, a la supervivencia de la empresa. Por voluntad propia o por necesidad –ojalá no- toda organización debe estar preparada para implantarlo.

He aquí algunas ventajas que proporciona implementar una adecuada política de ciberseguridad en el mundo de los negocios:

- **Garantía de la integridad** tanto de los datos como de los equipos de trabajo.

- **Mejora la imagen de marca y la confianza de los clientes.** Desde su origen, la actividad comercial se ha basado en las relaciones personales. Con el mismo origen, pero diferente formato, lo importante es que las partes confíen en la plataforma donde se está realizando el intercambio. Por otro lado, si una organización no es capaz de salvaguardar los datos, ¿qué garantía hay de que sí lo sea con sus productos o servicios?

- **Aumenta la productividad** al tener todos los equipos y redes en funcionamiento, sin detener la actividad, continúa el flujo de trabajo sin interrupciones, lo cual no ocurre si se detecta la presencia de un malware (programa malicioso) en algún dispositivo.

- **Ahorra gastos:** un ataque informático puede comportar gastos de reparación y recuperación, gastos que pueden ser muy importantes si, por ejemplo, se es víctima de un ataque de ransomware (secuestro de datos) en el que se nos exige un rescate.

- **Mayor capacidad de recuperación:** Una política de ciberseguridad incluye un procedimiento para la recuperación de nuestros datos en caso de que suceda un imprevisto.

- **Certeza de la veracidad de los datos contenidos en las empresas.** De nuevo volvemos al concepto de confianza del cliente hacia nuestra organización. Por otro lado, una fuga de datos producida por una deficiente política de ciberseguridad puede dar lugar a sanciones administrativas.

Y todo empieza por el principio: una **auditoría de ciberseguridad** realizada por profesionales permitirá saber en qué punto está una organización, qué nivel de protección tiene, cuáles son los puntos vulnerables y cuáles son sus necesidades.

A través de este catálogo de servicios de ciberseguridad podrás conocer las soluciones existentes en esta área que son prestadas por las empresas y profesionales de AERTIC. Te invitamos a conocerlos y consultarles tus posibles dudas.

aertic Agrupación Empresarial Innovadora del sector TIC de La Rioja

datalia
seguridad de la información

C/ Saturnino Ulargui, 2
26001 · Logroño · La Rioja

+34 941 23 41 10

datalia@datalia.info

www.datalia.info

ESPECIALIZACIÓN

Empresa de ciberseguridad con experiencia en diferentes sectores económicos

DIFERENCIACIÓN

Servicios con un enfoque eminentemente preventivo, con la finalidad de evitar riesgos y garantizar la continuidad de los procesos de los clientes. Acreditaciones en Sistemas de Gestión de Continuidad del Negocio - ISO 22301 – AENOR; Hacking Ético nivel I y nivel II – ThinkTIC y Análisis y gestión de riesgos ISO 31000 – ThinkTIC

DIRIGIDOS A

Empresas de diferentes tamaños y a entidades de la Administración.

PRODUCTOS Y SERVICIOS

Auditorías de seguridad: **Análisis de vulnerabilidades. Aplicaciones web**
Análisis de las aplicaciones para la detección de 'agujeros' que podrían suponer potenciales vulnerabilidades para los ciberatacantes.

Prevención ante el phising: **Concienciación. Empleados. Simulación**
Simulación de un ataque a través de correo electrónico para comprobar qué empleados están concienciados y poder darles formación previniendo así de los ataques de phishing.

Cifrado de información. **Contraseñas. Protección. Seguridad**
Instalación, configuración y formación de herramienta para generar contraseñas a archivos que puedan contener información sensible.

Bastionado de ordenadores. **Políticas. Configuración. Control**
Revisión de configuración de seguridad de dispositivos mediante la implantación de políticas de contraseñas, entre otras.

Cumplimiento normativo: **ISO 27001. ENS. RGPD. LOPD y GDD**
Asesoramiento para cumplir con la legislación vigente de protección de datos, obligatoria desde 2018 e identificación de las amenazas que pueden afectar a la seguridad de la organización. Implementación de medidas basadas en la norma ISO 27001 o de acuerdo al Esquema Nacional de Seguridad.

CASOS DE ÉXITO

- Auditorías de ciberseguridad en organizaciones y empresas.
- Auditoría informática en corporaciones locales.

EMESA grupo

C/ Saturnino Ulargui, 7
26001 · Logroño · La Rioja

+34 941 227 912

info@emesa.com

www.emesa.com

ESPECIALIZACIÓN

Implementación de servicios de ciberseguridad, incluyendo servicios de concienciación, auditoría y estudios de carácter forense.

DIFERENCIACIÓN

Contar con destacados partners tecnológicos, excelencia en la implementación de servicios y experiencia amplia en la actividad.

DIRIGIDOS A

Tejido industrial en general y empresas, tanto de sectores productivos como de servicios, con capacidad para atender las necesidades de empresas y organizaciones de diferente tamaño.

PRODUCTOS Y SERVICIOS

- SOC 24x7 (Detección, threat hunting, investigación, y Respuesta)
- Test de penetración y hacking ético
- Servicios de Red, Blue y Purple Team
- Detección de vulnerabilidades
- Seguridad de Aplicaciones
- Ciber Inteligencia
- CSIRT (Incident Response)
- Protección de entornos industriales / infraestructura crítica
- Protección de aplicaciones en Cloud (CASB)
- Servicio WAF
- Proxy Cloud
- EDR gestionado

COLABORACIONES Y PARTNERS

- SONICWALL
- FIRST (organización mundial de centros de Respuesta a Incidentes de Seguridad)
- APWG (Antiphising Working Group)
- Cyberark
- Fortinet
- Palo Alto
- Imperva
- McAfee
- Netskope
- Qualys
- Trend Micro
- Veracode

CASOS DE ÉXITO

- Gestión integral de la seguridad de empresa IBEX35: Gestión de más de 15.000 dispositivos, operación de seguridad 24x7 y alertas, gestión automatizada de cambios y respuesta a incidentes de seguridad.
- Servicios de SOC gestionados para Telco: Diseño, despliegue y definición de los procedimientos de gestión, servicio de correlación, threat hunting, despliegue de casos de uso específicos y capacidades de respuesta.

PROYECTOS RELEVANTES

- Despliegue de WAF en cloud para protección de red de sites corporativos (empresa IBEX35)
- Servicio de ciberinteligencia para la detección de fraude y riesgos.
- Proyecto de despliegue de plataforma de correlación de eventos de seguridad y analítica de seguridad en entornos OT.

mass SECURITY

Av. Gran Vía Juan Carlos I, 23, entpta. 2
26002 · Logroño · La Rioja

+34 941 26 31 47

central@mass-security.es

www.mass-security.es

ESPECIALIZACIÓN

Soluciones, integraciones personalizadas y proyectos integrales de seguridad física y Lógica (ciberseguridad), cumplimiento normativo y telecomunicaciones. Madrid y Valladolid.

DIFERENCIACIÓN

Empresas tecnológicas propias para el diseño de soluciones a medida, así como su experiencia en normativa

DIRIGIDOS A

Empresas, profesionales liberales, administraciones públicas y particulares que aspiran a implantar en el mercado una filosofía de seguridad integral, personalizada y de calidad.

PRODUCTOS Y SERVICIOS

Servicios de Ciber Seguridad.

Servicios de Cumplimiento Normativo (DP&Compliance).

Servicios de seguridad contra intrusión. CCTV.

Control de presencia y accesos.

Servicios contra incendios (Detección-Extinción).

Soluciones en Telecomunicaciones.

Soluciones SaaS y servicios CLOUD.

Planes de emergencias y evacuación con tecnología Virtuel360 (DP).

Normativa Food Defense e Industria 4.0. Servicios de Auditoría y consultoría.

COLABORACIONES Y PARTNERS

Panda, Walhalla, Risco, Aguilera, Global Cloud Factory, Axis, Aclatel-Lucent Entreprese, Hikvision, Tesa, Johnson Controls…

TECNOLOGÍAS Y METODOLOGÍAS

Disponen de certificaciones que avalan que todos los procesos están auditados por diferentes certificaciones, ISO 9001, ISO 14001, ISO 27001, IQNet, Empresa digna de confianza.

Empresa instaladora y mantenedora de sistemas contraincendios (PCI) CI025577.

Habilitación por la Dirección General de la Policía.

CASOS DE ÉXITO

Cadena de tiendas de telefonía Commcenter. Gestión de la dirección de seguridad de las más de 100 tiendas, implementando elementos físicos, lógicos y procedimentales, para la reducción de todas las incidencias.

PROYECTOS RELEVANTES

Desarrollo de cámara 360º para sistemas periciales en tráfico urbano. Patente y desarrollo de virtuale360. Soporte y asesoramiento plataforma de integración *Vida*.

Agrupación Empresarial Innovadora del sector TIC de La Rioja

SDi Digital Group

C/ Alfonso VI 4
26007 · Logroño · La Rioja

+34 941 13 50 52

info@sdi.es

www.sdi.es

ESPECIALIZACIÓN

Soluciones de gestión con integración de todas las áreas y departa¬mentos: ERP, páginas web, ecommer¬ce, marketing digital, app e interacción software con plataformas.

DIFERENCIACIÓN

Equipo de soporte altamente cuali¬ficado. Solucionadores de software. Adaptación de cualquier software a los requerimientos de la empresa. Tecnología y digitalización.

DIRIGIDOS A

- Empresas que quieren crecer gracias a la tecnología
- Optimización de procesos empre¬sariales a partir de su estrategia digital

PRODUCTOS Y SERVICIOS

Software: ERP y CRM para pymes, nóminas, recursos humanos para gran empresa, asesorías y despachos profesionales, gestión y contabilidad para pymes, DP Software verticalizado en todos los sectores empresariales.

HRLOG: Plataforma digital de fichajes y recursos humanos. DP Prestasync: Plataforma de conexión de ERP con ecommerce. DP. Desarrollo de páginas web y ecommerce. DPMarketing digital, seo, sem, estrategia digital. DPDiseño y fotografía de productos para entornos web. DP Desarrollo de plataformas digitales. DP Desarrollo de aplicaciones nativas Android, IOS. DP Proyectos de consultoría de software. DP Sistemas y soluciones en cloud. DP Soluciones de movilidad para comerciales. DPSAP Business One. Wolters Kluwer. ODOO ERP. HRLOG. Wordpress Nomina Clouda3 ERPa3Asesora3 Equipo. Prestashop .SEO .SEM .Adwords.

COLABORACIONES Y PARTNERS

- PrestaShop - Partner Platinium.
- Wolters Kluwer - Partner Gold.
- Partner EcosystemODOO - Partner AEODOO.
- Google.

TECNOLOGÍAS Y METODOLOGÍAS

.Net Sql MySql Symfony Bootstrap HTML5 IOS Android Ionic Adobe Python Odoo SAP Business One Jira PrestaShop Wordpress Agile Scrum Git.

CASOS DE ÉXITO

Hemos conseguido en varios de nuestros clientes que no tenían presencia en internet, que facturen en tan sólo dos años más de 1.000.000 € por su nueva plataforma ecommerce que hemos habilitado y que hemos sincronizado con sus sistemas de gestión y ERP. Ahora puede ofrecer a sus clientes y proveedores información en tiempo real de sus stocks, pedidos y toda la información relevante. Además como la información del ERP la tiene unificada con la web, puede ofrecer a cada cliente experiencias de compra personalizada.

PROYECTOS RELEVANTES

Proyecto de digitalización de varios sectores empresariales y desarrollo de software que se ha implantado en más de 1.000 empresas.

Agrupación Empresarial Innovadora del sector TIC de La Rioja

Plaza Villafranca de los Barros, 2
28034 · Madrid

+34 91 123 11 73

lorenzo@securizame.com

www.securizame.com

ESPECIALIZACIÓN

Ciberseguridad.

DIFERENCIACIÓN

Su especialización, el conocimiento y experiencia real y su agilidad son rasgos distintivos. Sistema de trabajo que genera confianza y tranquilidad a sus clientes, para hacerles saber que están en manos expertas en ciberseguridad.

DIRIGIDOS A

Diferentes sectores como son el energético, tecnológico, legal, retail,comunicaciones, ingeniería, medios de información, etc, que desean centrarse en su actividad y dejar la seguridad en manos expertas.

PRODUCTOS Y SERVICIOS

Asesoría en ciberseguridad

Auditoría técnica en ciberseguridad y Hacking ético (pentesting)

Peritaje informático forense

Respuesta ante incidentes de seguridad

Integración

Gestión y operación de soluciones de seguridad

Formación especializada en ciberseguridad (Hacking ético, Análisis forense y Respuesta ante Incidentes) y scripting en Python

Sistemas de backup a prueba de ransomware (DP)

Gestión de monitorización de sistemas remotos (DP)

Entrenamientos 100% prácticos en respuesta ante incidentes y análisis forense (DP)

Certificaciones de ciberseguridad 100% prácticas: IRCP y RTCP (DP).

CIBERSEGURIDAD

Agrupación Empresarial Innovadora del sector TIC de La Rioja

grupoPancorbo SISTEMAS
INFORMÁTICA Y REPROGRAFÍA

C/ Rafael Azcona 6
26005 · Logroño · La Rioja

+34 941 20 33 77

info@sistemasinformatica.com

www.sistemasinformatica.com

ESPECIALIZACIÓN

Consultoría, implantación de soluciones de ciberseguridad (cortafuegos, endpoint, backups resilientes). Concienciación y formación a usuarios finales.

DIFERENCIACIÓN

Equipo de trabajo muy capacitado por experiencia y formación. Incorporación de jóvenes talentos. El consultor y el técnico preventa realizan un trabajo junto con el fabricante para aportar la mejor solución. Dispone de las últimas tecnologías.

DIRIGIDOS A

Empresas con necesidades en ciberseguridad y protección.

SERVICIOS

Consultoría. Auditoría. Despliegue de soluciones de protección de perímetro y endpoints. Despliegue de tecnologías de backups.

Soluciones para pymes

Firewalls. Endpoints. Backups Resilientes on premise y en la nube.

COLABORACIONES Y PARTNERS

Sophos. Dell Tecnologies.

TECNOLOGÍAS Y METODOLOGÍAS

Sophos. Datadomain powerprotect. PMI.

CASOS DE ÉXITO

- Empresa referente en el sector de energías renovables: securización y adecuación de sus comunicaciones entre sedes repartidas por todo el mundo.
- Empresa puntera del sector del calzado: protección de su red, wifi, procesos de fabricación.
- Centros tecnológicos: securización de su entorno

PROYECTOS RELEVANTES

Proyectos de securización en diferentes sectores empresariales.

CIBERSEGURIDAD

Agrupación Empresarial Innovadora del sector TIC de La Rioja

SSH TEAM CONSULTING

C/ Tirso de Molina 10
26006 · Logroño · La Rioja

+34 669 468 889

cprieto@sshteam.com

sshteam.com

ESPECIALIZACIÓN

Ciberseguridad: Auditoría, diagnóstico, pentesting, TOTALSOC.

DIFERENCIACIÓN

Experiencia con grandes empresas y servicios de ciberseguridad especializados. Partners de reconocido prestigio. Alianzas sólidas comerciales locales y nacionales. Productos desarrollados para Pymes. Equipo multidisciplinar con certificaciones como OSCP, CEH, AWAE, CISA, CISM, Lead Auditor 27001

DIRIGIDOS A

Pymes (especializados en el sector industrial) y grandes empresas.

PRODUCTOS Y SERVICIOS

Auditorias y diagnósticos de seguridad a través de pentesting para entornos IT / OT. Pentesting Web. Grado de Madurez. Wi-Fi. Código y desarrollo seguro. Consultoría Tecnológica. Proyectos 'llave en mano' con enfoque. Consultoría Compliance. ISO 27001. Esquema Nacional de Seguridad. Peritajes e informes periciales. Formación y Concienciación.

Soluciones para pymes

Gestión Automatizada de Ciberseguridad. TOTALSOC

COLABORACIONES Y PARTNERS

Ofrecen herramientas automatizadas para la realización de auditorías tecnológicas, como Nessus, Acunetix, etc. Realizan el desarrollo de software con una visión de desarrollo seguro y metodologías agiles. Tecnologías y metodologías.

CASOS DE ÉXITO

- **Oficina Técnica de Seguridad.** Integrados en departamentos de ciberseguridad de grandes empresas (audiovisual, banca, seguridad física, etc.)
- **Auditorias Tecnológicas para distintos sectores industriales** (agroalimentario, bodegas, aeroespacial, tecnológico, litografía, etc)

PROYECTOS RELEVANTES

- NEOTEC. A través de CDTI, proyecto de innovación tecnológica
- Cibersecurity Ventures. Grupo de 10 empresas aceleradas por INCIBE
- BFFood. Clúster agroalimentario para aceleración de startups tecnológicas.

GLOSARIO

31 términos imprescindibles para vivir más seguros

ADWARE/MALVERTISING
Es un programa que muestra automáticamente publicidad al usuario, bien sea durante la instalación o durante el uso. El beneficio es para los creadores. No es forzosamente Malware ("software malicioso", término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas) ya que en ocasiones es un medio legítimo empleado por desarrolladores. Ejemplo: demos o versiones de prueba en las que la publicidad desaparece al adquirir la licencia.

AGUJERO DE SEGURIDAD
Se trata de deficiencias de un programa que pueden permitir a terceros a acceder a información de modo no legítimo. Las empresas deben llevar un control periódico para detectar estos agujeros.

ANTIVIRUS
Software de protección para evitar que ejecutemos algún tipo de software malicioso en nuestro equipo que infecte al mismo.

AUDITORÍA DE SEGURIDAD
Estudio cuya finalidad es identificar las diversas vulnerabilidades que pudieran presentarse en las estaciones de trabajo, servidores, aplicaciones o redes de comunicaciones. Lo realizan profesionales en tecnología de la Información.

AUTENTICACIÓN
Forma de comprobar que alguien es quien dice ser cuando opera o accede a un servicio online.

BACKDOOR (PUERTA TRASERA)
Un concepto muy conocido por las películas y literatura sobre el tema. Es un punto débil de un programa que permitiría acceder de forma ilegítima a una persona no autorizada. Se trata de una idea muy cercana a la de agujero de seguridad. Se caracterizan por tener una codificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea, http, ftp, telnet o chat. En ocasiones, la puerta trasera la generan los propios creadores del programa.

BACKUP (COPIA DE SEGURIDAD)
Copia de los datos y programas de un ordenador que se realiza con la finalidad de recuperar datos en caso de que se produzca una circunstancia imprevista. Puede realizarse sobre soportes físicos (discos duros, discos ópticos, USB o DVD) o en la nube. Conviene realizar el procedimiento periódicamente.

BOMBA LÓGICA
Fragmento de código que se inserta en un programa intencionadamente. Al contrario que un virus, la bomba lógica permanece inactiva hasta que se realizan unas acciones previamente programadas. Es entonces cuando se desarrolla la acción maliciosa.

BOT (ZOMBIE)
Así se denomina a un ordenador dominado remotamente por un ciberdelincuente, quien se ha hecho con el control tras una infección por malware. El ciberdelincuente puede emplear el ordenador infectado para realizar acciones ilícitas.

BUG (ERROR DE SOFTWARE)
Es un fallo de programa que tiene como consecuencia un resultado no deseado.

CERTIFICADO DIGITAL
Fichero informático que sirve para confirmar una identidad en internet. Lo genera una autoridad certificadora y asocia unos datos a una persona física, organismo o empresa.

CLOUD COMPUTING (COMPUTACIÓN EN LA NUBE)
Permite el almacenamiento de ficheros, información y datos en servidores ajenos, de modo que puedan estar disponibles en cualquier dispositivo. Requiere una especial atención en cuanto a la seguridad de la información ya que contiene datos personales e información sensible almacenada en servidores de terceros, por lo que puede ser hackeada.

CORTAFUEGOS (FIREWALL)
Sistema de seguridad (compuesto por programa o dispositivos) que tiene como objeto impedir los accesos no autorizados.

CRIPTOGRAFÍA
Técnica que permite cifrar un mensaje convirtiéndolo en ilegible para quien no conozca el código.

CRL (LISTA DE REVOCACIÓN DE CERTIFICADOS)
Las listas de revocación de certificados permiten verificar la validez de un certificado digital a través de listas emitidas por las autoridades oficiales de certificación. Se renuevan cada 24 horas.

FIRMA ELECTRÓNICA
Es el conjunto de datos electrónicos que están asociados a un documento electrónico. Debe identificar al firmante, verificar la integridad del documento firmado, garantizar el no repudio en el origen, contar con la participación de un tercero de confianza y estar basada en un certificado electrónico reconocido.

FUGA DE DATOS
Se define como cualquier pérdida de la confidencialidad de la información privada de una persona o empresa.

GUSANO
Un tipo de programa malicioso que se caracteriza por su dispersabilidad. Realiza copias de sí mismo y continúa propagándose e infectando ordenadores sin necesidad de la acción humana.

HACKER
Se denomina así a la persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.

IDS (Intrusion Detection System)
El IDS es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red. Solo detecta estos accesos, no los previene.

IPS (Sistema de Prevención de Intrusos)
Es un software que sirve para proteger a los sistemas de ataques y abusos. Por su naturaleza, se considera cercano a los cortafuegos.

LAN (RED DE ÁREA LOCAL)
Es una red de pequeño ámbito geográfico. Suele comprender una oficina, una vivienda o un edificio. Pueden ser cableadas (más rápidas y seguras) o inalámbricas (menos seguras, pero permiten la movilidad de dispositivos)

MALWARE
Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información, siempre con intención dañina o lesiva. Un malware puede ser un virus, gusano, troyano, backdoor, spyware…

PHARMING
Tipo de ataque informático que consiste en suplantar la IP legítima de una entidad de modo que cuando un usuario escribe en la barra de direcciones una dirección web, es redirigido a una web falsa que suplanta a la auténtica. De este modo, el ciberdelincuente puede obtener las claves de acceso del usuario.

PHISING
Estafa que consiste en intentar obtener de forma fraudulenta los datos (normalmente bancarios) de usuarios legítimos. Puede realizarse vía e-mail, SMS, o por llamada telefónica y la finalidad es aparentar una comunicación oficial y de confianza que convenza a la víctima de aportar sus datos (claves de acceso, número de tarjeta, PINs…).

PLAN DE CONTINGENCIA TIC
Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) es una estrategia planificada en fases. Está constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación. Su objetivo es conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en la compañía.

PROXY (GATEWAY)
Dispositivo y/o programa que hace de intermediario entre los equipos de una red de área local e internet. Puede proporcionar algunos servicios de seguridad (cortafuegos) que impidan accesos no autorizados desde el exterior.

RAMSONWARE (SECUESTRO DE DATOS)
Es la toma de control de un ordenador y cifrado de todo su contenido de modo que se convierte ilegible si no se cuenta con la clave de cifrado correspondiente. Normalmente, el ciberdelincuente exige una cuantía monetaria (rescate) al propietario de equipo para facilitar la clave y poder acceder a sus datos.

RED PRIVADA VIRTUAL (VPN)
Es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet. Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autenticación y el cifrado.

SPYWARE (PROGRAMA ESPIA)
Programa malicioso que recopila información de un ordenador que luego se envían a una entidad remota.

TROYANO
Se trata de un tipo de malware o software malicioso que no se autorreplica. Generalmente, este tipo de malware requiere del uso de la ingeniería social para su propagación. Una de las características de los troyanos es que al ejecutarse no se evidencian señales de un mal funcionamiento; sin embargo, mientras el usuario realiza tareas habituales en su ordenador, el programa puede abrir diversos canales de comunicación con un equipo malicioso remoto que permitirán al atacante controlar el sistema de una forma absoluta.

* Términos y definiciones basadas en el "Glosario de términos de ciberseguridad. Una guía de aproximación para el empresario", publicado por INCIBE (Instituto Nacional de Ciberseguridad)