Ley de Internet

Seguridad e Industria 4.0

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Index

Lista de abreviaciones

APT: Advanced Persistent Threats (Amenazas persistentes avanzadas)

CERT: Computer Emergency Response Team (Equipo de respuesta ante emergencias informáticas)

CNCS: Centro Nacional de Cibersegurança (Centro Nacional de Cibersegurança)

CSC: Cyber Security Center (Centro de seguridad cibernética)

CSIRT: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad informática)

DDOS: Distributed Denial of Service (Denegación de servicio distribuida)

DSN: Digital Supply Network (Red de suministro digital)

EU/UE: European Union/ Unión Europea

GDPR: General Data Protection Regulation (Reglamento general de protección de datos)

ICT/TIC: Information and Communication Technology/ Tecnología de la información y la comunicación

IDSA: Czech Institute of Informatics, Robotics and Cybernetics (Instituto checo de informática, robótica y cibernética)

IT/ TI: Information Technology/Tecnología de la información

ÖSCS: Österreichischen Strategie für Cyber Sicherheit

NCBI: NarodniCentrumBezpecnejsiholInternetu

SIC: Safer Internet Center (Centro de Internet más seguro)

SME/PYME: Small and Medium ENterprise/Pequeñas y Medianas Empresas

Figures

Key definitions

Amenazas Persistentes Avanzadas: ataques conplejos y dirigidos contra infraestructuras críticas de TI de empresas y autoridades públicas.

Botnet: colección de dispositivos conectados a internet que pueden incluir ordenadores, servidores, dispositivos móviles y dispositivos de iternet de las cosas que son infectados y controlados por un tipo común de *malware*.

Ciberseguridad: La práctica de proteger sistemas, redes y programas de ataques digitales. Estos ciberataques tienen como objetivo ,generalmente, acceder cambiar o destruir información sensible, extorsionar a los usuarios a cambio de dinero o interrumpir los procesos normales de negocio.

Violaciones de datos: una divulgación intencional o no intencional de información segura o privada/confidencial a un entorno no confiable. Las violaciones de datos pueden involucrar información de salud personal, información de identificación personal, secretos comerciales y/o propiedad intelectual.

Ataque de denegación de servicio: un evento de seguridad que ocurre cuando un atacante impide que los usuarios legítimos accedan a sistemas informáticos, dispositivos, servicios u otros recursos de TI específicos.

Seguridad en Internet: conocimiento a cerca de la seguridad personal del usuario y los riesgos en la información privada y propiedad asociada con el uso de Internet y la autoprotección contra el delito informático en general.

Carta falsa/cadena: un informe falso que se transmite por correo electrónico, mensajería instantánea, redes sociales u otros medios. Los engaños maliciosos están destinados a atraer

a los usuarios a las trampas mediante el envío de enlaces prometedores adicionales que, sin embargo, solo causan virus o malware o conducen a sitios web fraudulentos.

Malware: cualquier programa o archivo que sea dañino para un usuario del ordenador. Los tipos de malware pueden incluir virus informáticos, gusanos, troyanos y *spyware*. Estos programas maliciosos pueden realizar una variedad de funciones diferentes, como robar, cifrar o eliminar datos confidenciales, alterar o secuestrar funciones informáticas centrales y monitorear la actividad del ordenador de los usuarios sin su permiso.

Phishing: es una forma de fraude en el que un atacante se hace pasar por una entidad o persona de buena reputación en un correo electrónico u otros canales de comunicación. El atacante usa correos electrónicos de *phishing* para distribuir enlaces maliciosos o archivos adjuntos que pueden realizar una variedad de funciones, incluida la extracción de credenciales de inicio de sesión o información de cuenta de las víctimas.

Ransomware: software malicioso que tiene como objetivo bloquear el acceso a archivos y sistemas que requieren el pago de un valor para devolver el acceso.

Difamación: declaración falsa sobre alguien que daña su reputación.

Spam: sistemas de mensajería electrónica para enviar mensajes no solicitados o no deseados a granel. La forma más común de correo no deseado es el correo electrónico, pero el término también se aplica a cualquier mensaje enviado electrónicamente que no se haya solicitado y en masa.

Troyano: tipo de *malware* que a menudo se disfraza de *software* legítimo. Puede ser empleado por ciber-ladrones y *hackers* que intentan acceder a los sistemas de los usuarios.

Virus: un virus informático es un tipo de código o programa malicioso escrito para alterar el funcionamiento de un ordenador y está diseñado para propagarse de uno a otro.

Warez: software pirateado (como por ejemplo la copia ilegal), a menudo después de la desactivación de las medidas contra la privacidad que se distribuyen a través de Internet.

Gusano: tipo de programa de *software* malicioso cuya función principal es infectar otros ordenadores mientras permanece activo en los sistemas infectados.

1. Introducción

La Industria 4.0 promoverá varios cambios en las empresas, ya que afectará a todos los niveles de producción y cadenas de suministro, incluidos los gerentes de negocios y producción, trabajadores, sistemas ciberfísicos, clientes, entre otros, así como a los ciudadanos en su vida privada.

Aunque la cantidad de beneficios que surgen con la Industria 4.0, la información y los activos que poseen o utilizan las organizaciones y las personas se vuelven cada vez más importantes. Debido a esto, con la nueva revolución industrial, la existencia de ataques aumenta exponencialmente y también trae nuevos riesgos que deben considerarse y abordarse tanto para las organizaciones como para la sociedad en general.

Por lo tanto, la ciberseguridad debería convertirse en una parte integral de la estrategia, el diseño y las operaciones, y la implementación de medidas es muy importante a partir de ahora. Hay muchas medidas/prácticas para implementar en las empresas y en la vida privada de los ciudadanos con el fin de mejorar la seguridad y la seguridad para recopilar, proteger y proporcionar información. Además, aunque existen algunas iniciativas e instituciones involucradas en la seguridad de Internet, todavía hay mucho trabajo por hacer, especialmente porque el mundo actual es extremadamente dinámico y, como consecuencia, siempre surgen nuevas amenazas, se descubren nuevas vulnerabilidades y la falta de desarrollo/capacitación de los trabajadores es un desafío clave.

La nueva era de la digitalización está trayendo el uso creciente de tecnologías digitales en aún más áreas de negocios y sociedad y la creciente conectividad de todo. Esta situación también es responsable de importantes desafíos socioculturales, económicos, mayores retos y amenazas en el nivel de seguridad y algunos cambios de política en el territorio europeo. Teniendo esto en cuenta, es absolutamente necesario hacer que la sociedad sea más consciente y esté más preparada para esta realidad e incluir algunas estrategias a nivel nacional para ayudar a lograr una comunidad más segura a nivel mundial a diario.

En este informe, tenemos una breve descripción de los principales desafíos que enfrentan las personas todos los días en algunos países europeos, los principales riesgos/dificultades y los incidentes más comunes con respecto a la ciberseguridad y a la seguridad.

2. Industria 4.0: una breve reseña

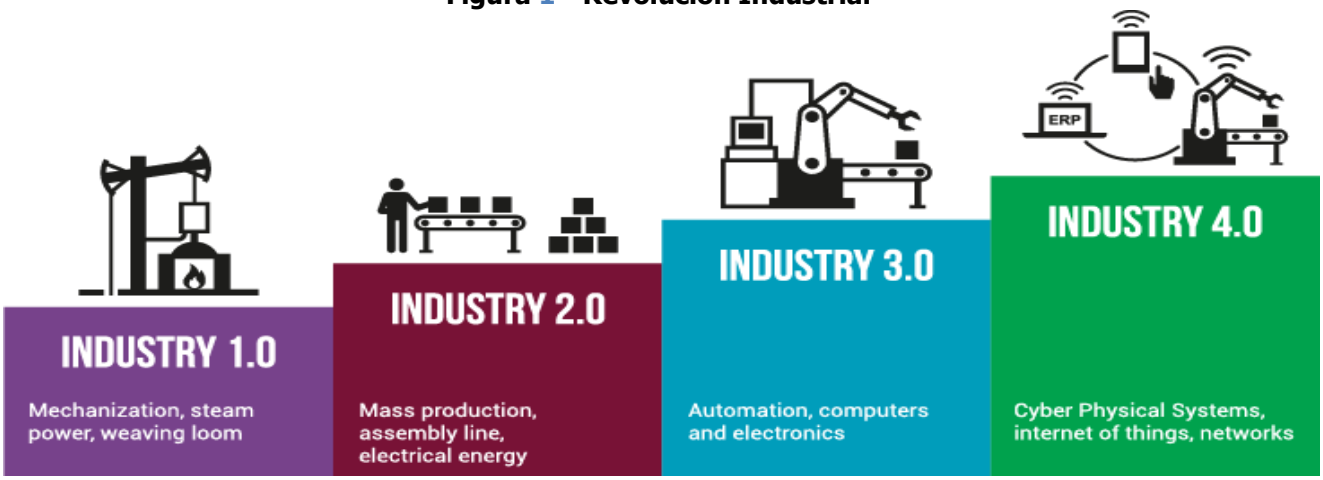
La Cuarta Revolución Industrial, comúnmente conocida como Industria 4.0, se caracteriza por la inteligencia descentralizada que ayuda a crear redes de objetos inteligentes y gestión de procesos independiente, con la interacción de los mundos real y virtual que representa un nuevo aspecto crucial de los procesos de fabricación y producción.

De hecho, la industrialización del mundo comenzó a finales del siglo XVIII con la Primera Revolución Industrial y se definió por la introducción de instalaciones de producción mecánica con la ayuda de agua y vapor.

La Cuarta Revolución Industrial se caracteriza por la transformación digital con el desarrollo de tecnologías ciberfísicas que permiten cambios disruptivos en los modelos de producción y de negocio.

La Industria 4.0 es una consecuencia natural de la tercera revolución industrial que transformó completamente la naturaleza del comercio en la segunda mitad del siglo XX con una serie de avances en informática y tecnología de la información (TI). Fue un período de grandes cambios para las empresas minoristas y de bienes de consumo, marcado por la aparición de tarjetas de crédito, automatización de oficinas acministrativas y almacenes, cadenas de suministro justo a tiempo y los primeros modelos de negocio en línea. De hecho, el concepto de Industria 4.0 es relativamente reciente y ha crecido en importancia durante los últimos años dentro de las diferentes compañías.

Figura 1 - Revolución Industrial



Fuente: (Simio, n.d.)

La industria 4.0 es una combinación de varios avances tecnológicos:

- **Tecnología de la información y la comunicación:** la digitalización y la aplicación generalizada de la Tecnología de la Información y la Comunicación (TIC) permiten la integración de todos los sistemas a lo largo de las cadenas de suministro y valor y permiten la agregación de datos en todos los niveles. La información se digitaliza y los sistemas correspondientes dentro y entre las compañías se integran en todas las etapas de la creación de productos y los ciclos de vida de uso;

- **Sistemas ciberfísicos:** los sistemas ciberfísicos mejoran la capacidad de controlar y monitorear procesos físicos, con la ayuda de sensores, robots inteligentes, drones, dispositivos de impresión 3D (algunos de los cuales se detallarán más en este informe). En los sistemas ciberfísicos, los componentes físicos se agregan en una red de elementos que interactúan. Mientras que las entradas iniciales y las salidas finales son habitualmente físicas, la información a menudo se transpone entre estados físicos y digitales durante el proceso de fabricación;

- **Comunicación de red:** todos estos dispositivos, tanto dentro de la planta de fabricación como a través de proveedores y distribuidores, están conectados a través de diferentes tecnologías inalámbricas e Internet. Las redes de comunicación confiables y de alta calidad son un requisito crucial de la Industria 4.0 y, por lo tanto, es importante expandir la infraestructura de Internet de banda ancha donde sea necesario. Este alto nivel de conexión en red de componentes interconectados permite un funcionamiento descentralizado y autoorganizado de los sistemas ciberfísicos;

- **Big data y cloud computing:** con el uso de big data y cloud computing, la información recuperada a través de estas redes puede utilizarse para modelar, virtualizar y simular productos y procesos de fabricación;

- **Modelado, virtualización y simulación:** la simulación es una funcionalidad central de los sistemas mediante una asistencia continua a lo largo de todo el ciclo de vida, por ejemplo, mediante el soporte de la operación y el servicio con un enlace directo a los datos de la operación;

- **Herramientas mejoradas para la interacción y la cooperación humano-ordenador:** para controlar estos procesos, la fuerza laboral humana cuenta con herramientas TIC de última generación que hacen uso de los avances en realidad aumentada y robótica inteligente. Los sistemas ciberfísicos de la Industria 4.0 tienen el objetivo principal de ayudar a los humanos en sus trabajos cotidianos. Las características clave de tales sistemas son la no intrusión, la adaptación al contexto, la personalización, la ubicación y la movilidad.

Además, es importante tener en cuenta que también hay algunos desafíos importantes asociados con la Industria 4.0 y la seguridad en Internet. Los dos principales desafíos importantes son:

- Seguridad: Quizás el aspecto más desafiante de la implementación de técnicas de la Industria 4.0 es el riesgo de seguridad de las TI. Esta integración en línea dará espacio a violaciones de seguridad, fugas de datos e incluso podría implicar el robo cibernético. A medida que se recopilen datos a lo largo de la cadena de suministro, surgirán cuestiones de propiedad y es importante que las empresas se aseguren de que sus datos no terminen en manos de un competidor. Por otro lado, debe garantizarse que las instalaciones de producción en sí mismas no representen una amenaza para los humanos o el medio ambiente circundante y que los trabajadores reciban capacitación continua en seguridad;

- **Privacidad:** este problema concierne no solo a los clientes sino también a los productores. Por un lado, el cliente necesita recopilar y analizar datos relevantes para el desarrollo de su negocio. Por otro lado, el cliente podría sentir que su privacidad está siendo amenazada. Además, las pequeñas y grandes empresas que no han

compartido sus datos en el pasado tendrán que trabajar para lograr un entorno más transparente. Cerrar la brecha entre el consumidor y el productor será un gran desafío para ambas partes.

2.1. ¿En qué medida se ha adaptado la Industria 4.0 a los desafíos creados por la seguridad en Internet en su país?

2.1.1. Austria

El concepto de Industria 4.0 impulsa la conexión en red de máquinas a través de Internet y, por lo tanto, abre los sistemas previamente cerrados a nuevos peligros como los ciberataques o *malwares*. La protección de los sistemas de TI requiere un concepto de seguridad integral y una gestión estratégica de la seguridad de la información.

La asociación "Platform Industry 4.0" es consciente de la importancia del aspecto de seguridad en relación con la Industria 4.0 y recientemente identificó el enfoque "Seguridad y protección" en la reunión de estrategia de 2017.

Con el establecimiento del grupo de expertos "Security and Safety", la plataforma Industria 4.0 Austria quiere aumentar la percepción de la importancia y el significado del tema Seguridad para la Industria 4.0, establecer redes de actores relevantes en Austria y contribuir a establecer la Seguridad y Seguridad como una ventaja competitiva austriaca . Los miembros y expertos interesado de la investigación y la industria contarán con un foro para el intercambio de experiencias y la oportunidad de desarrollar una comprensión común de la seguridad en relación con la digitalización. Como primeros proyectos conjuntos, se planifica la creación de un catálogo de ciencias de competencia en seguridad en toda Austria, instituciones privadas de investigación y empresas, así como una directriz de "seguridad industrial" para empresas, con el objetivo de sensibilizar especialmente a las pequeñas y medianas empresas (PYME) sobre el tema para señalar puntos críticos en el área de seguridad y protección en las decisiones comerciales y ofrecer una primera asistencia.

La implementación de la Industry 4.0 no es posible sin garantizar la seguridad de los datos y el software. Por lo tanto, es necesario utilizar las normas internacionales de seguridad existentes, que permiten realizar pruebas profesionales de los sistemas y software utilizados,

además del desarrollo adicional de los sistemas de seguridad relevantes para la Industria 4.0. La seguridad de las TI en la Industria 4.0 adquiere un significado especial con el uso intensivo de Internet también para funciones de control de automatización, virtualización y computación en la nube, a través de tecnologías SelfX (autoconfiguración, autocuración, autooptimización) y la red basada en agentes de funciones inteligentes entre sí.

La familia estándar ISO / IEC 27000ff (desarrollada en ISO / IEC JTC 1 / SC 27, Técnicas de seguridad de TI) ofrece además de un sistema de gestión genérico para la seguridad de la información, una variedad de herramientas generalmente aceptadas y probadas en el campo y soluciones específicas de temas. como ISO / IEC 27036-4 para seguridad en servicios en la nube.

La norma IEC 62443 "Redes de comunicación industrial: seguridad de redes y sistemas" desarrollada en IEC / TC 65, Medición, control y automatización de procesos industriales, se basa en la familia de normas ISO / IEC 27000 (Verein Industrie 4.0 Österreich, 2016).

Por lo tanto, podemos confirmar que en Austria existen múltiples iniciativas que apuntan a mejorar los desafíos impuestos por la Industria 4.0. y seguridad en internet.

2.1.2. República Checa

En el caso de la República Checa, la Industria 4.0 moverá el negocio principal de la mayoría de las empresas al mundo digital. Los principales desafíos identificados en las empresas en la República Checa son los siguientes:

- **Seguridad de TI y confiabilidad de los sistemas clave:** en una empresa administrada por máquinas, será esencial que los datos de los sensores individuales dentro de las máquinas sean verdaderamente auténticos. Además, es importante que la configuración de la red no se vea comprometida. Las empresas se vuelven dependientes de su infraestructura de TIC;
- **Integridad del proceso empresarial:** la presión sobre el precio más bajo y el menor tiempo para implementar cambios en el proyecto dentro de la Industria 4.0 puede conducir a un efecto negativo. La configuración incorrecta del proceso puede ser esencial en la producción y entrega. Estos problemas pueden conducir a una pérdida financiera o incluso a problemas existenciales de la empresa;

- **Sensibilidad a las desperfectos de software:** en muchas empresas, el proceso de producción depende en gran medida del software, pero aún hay participación de personas involucradas en la operación del equipo. Además, las máquinas o líneas suelen funcionar de forma autónoma (no vinculadas al sistema global). En el futuro, las máquinas serán administradas por un software central, que dependerá del funcionamiento de los sistemas operativos, firewalls, protección IDS / IPS, herramientas de administración, etc.

2.1.3. Portugal

En Portugal hay algunas iniciativas en los últimos años para promover la Industria 4.0 en las empresas. En este contexto, el gobierno nacional en Portugal tiene un programa llamado "i4.0" que tiene como objetivo promover la reindustrialización nacional. Esta estrategia tiene más de 50 medidas públicas y privadas y las estadísticas dicen que estas medidas tendrán un impacto en más de 50,000 empresas que operan en Portugal y, en una fase inicial, permitirán la recalificación y también el desarrollo de competencias digitales de más de 20.00 trabajadores. Además, los principales desafíos de las empresas portuguesas con respecto a la adaptación a la Industria 4.0 y la seguridad en Internet son:

- **La falta de competencias digitales y la recalificación de los recursos humanos** y estos factores están contribuyendo al retraso del desarrollo de la transformación digital, el desarrollo de la madurez digital y pueden promover algunos riesgos de seguridad;
- La **falta de recursos humanos capaces de planear, ejecutar y garantizar la implementación y el mantenimiento de las soluciones de la Industria 4.0**. Para resolver esta situación, los gerentes de las empresas pueden desarrollar asociaciones con organizaciones externas, escuelas secundarias o técnicas y universidades;
- La **falta de capacidades y competencias para detectar fallos de seguridad** y cómo resolverlas. Con respecto a este tema, la mayoría de las empresas reconocen que necesitan implementar medidas/planes de seguridad porque con esto promoverán un proceso de transformación digital;

- La **reconversión de los sistemas antiguos a las tecnologías de la Industria 4.0 puede traer algunos riesgos de seguridad** porque los sistemas antiguos no están diseñados para tener un nivel tan alto de conectividad. Esto significa que para gestionar los riesgos de seguridad, las empresas deben garantizar la protección de sus sistemas, deben ser conscientes de evitar nuevas amenazas, deben ser resistentes para limitar algunos daños y reiniciar sus operaciones. Por lo tanto, cuando las empresas están estableciendo una estrategia para la Industria 4.0, todos los temas relacionados con la seguridad deben estar entre las principales prioridades.

2.1.4. España

En el caso de España, la creación de un entorno de confianza digital que permita reforzar la protección de las instituciones y promueva la implicación de los ciudadanos en el entorno digital es vital para el desarrollo de una sociedad conectada. Para lograr esta seguridad cibernética, la industria debe actuar como el elemento habilitador clave.

En relación con esto, la Agencia Digital Española, centrada en el objetivo antes mencionado y, en particular, a través del Plan Digital Trust, está estudiando la posibilidad de realizar un estudio de viabilidad en colaboración con los principales agentes de referencia y con el Foro Nacional para la Confianza digital con el propósito de desarrollar una propuesta de integración para poner en marcha una Industria de Ciberseguridad.

Después de la implementación del GDPR, el objetivo no es otro que garantizar un entorno más seguro para los datos personales y la información. Sin embargo, este proceso ha sido un desafío para las empresas. El nuevo estándar introduce herramientas como el derecho a ser olvidado, la obligación de informar en un lenguaje conciso, inteligible y simple o el hecho de facilitar la portabilidad de datos a otra compañía asignada sin ningún obstáculo. En particular, el desarrollo tecnológico está asociado con una mayor exposición a nuevas amenazas, particularmente aquellas asociadas con el ciberespacio. La hiperconectividad del mundo de hoy exacerba algunas de las vulnerabilidades del sistema de seguridad y requiere una mayor protección de las redes y sistemas, así como la privacidad y los derechos digitales del público. España debe adaptarse a esta transformación permanente intensificando sus esfuerzos para

digitalizar y tecnificar al Estado y la sociedad, basándose en un sistema educativo y de formación adaptado a esta nueva realidad.

Para adaptarse al cambio requerido por el nuevo Reglamento Europeo de Protección de Datos, ha sido necesario elaborar un plan desarrollado dentro de una Estrategia Nacional de Ciberseguridad que ha implicado un cambio enorme en las relaciones entre empresas, ciudadanos e instituciones públicas para promover El desarrollo de la sociedad. Esto ha sido posible mediante la creación de:

- **Plan Estratégico de Ciberseguridad:** El objetivo principal de este plan estratégico del Gobierno español se centra en garantizar un uso seguro de los sistemas y redes de información a través de un sistema de prevención, análisis, recuperación y detección de cualquier ciberataque en el campo de las Nuevas Tecnologías. De esta forma, la legislación nacional se cumple con la normativa establecida en el marco del derecho internacional de conformidad con los compromisos contraídos por España. Por otro lado, los desafíos de lograr una respuesta global, completa y flexible se centran en los riesgos y amenazas identificados.

- **Regulaciones y normas de seguridad:** tal como se define desde Europa, la protección de datos estará regulada y será obligatoria a partir del 25 de mayo de 2018. Establece la implementación de nuevas medidas de seguridad para autónomos, empresas y la administración pública. Estas medidas incluyen la implementación de encriptación y sistemas de autenticación básica de doble factor si el nivel de riesgo lo requiere. En este sentido, es crucial adaptarse a la LOPD y conocer el contenido de LSSICE, así como ayudar a una consultoría de protección de datos para verificar cómo se implementan las medidas de seguridad de la computadora y saber qué nivel de seguridad y protección debe garantizar contra cualquier ataque.

- **Regulaciones generales de protección de datos:** El derecho de Nuevas Tecnologías representa un gran avance en términos de documentación, pero debemos entender que estamos viviendo una nueva realidad conceptual y legal. Por otro lado, por medio de ataques informáticos, se debe considerar que una gran cantidad de

información confidencial puede ser robada diariamente. Las empresas han implementado herramientas preventivas y de protección para evitar que cualquier intruso acceda a su información. En resumen, el Reglamento general de protección de datos establece que las empresas deben informar los intentos de intrusión y el acceso no autorizado exitoso, así como los datos afectados. Estas medidas de ciberseguridad garantizan un mayor control y protección de la información privada.

- Algunos desafíos tecnológicos/sistémicos/organizacionales son:
  - **Mejora de las capacidades de ciberseguridad** de gobiernos, agencias públicas, organizaciones, universidades, etc., para avanzar y alcanzar el estado de la técnica en Ciberseguridad industrial;
  - **Aumentar la conciencia general y proporcionar capacitación especializada** adecuada para cada tipo de usuario;
  - **Desarrollo de herramientas para facilitar las alianzas público-privadas** a todos los niveles;
  - Aumentar la investigación sobre ciberseguridad industrial;
  - **Desarrollo de estrategias de ciberseguridad** para la industria;
  - **Desarrollo de pautas de mejores prácticas** y estándares de referencia;
  - **Fundación de laboratorios de prueba;**
  - **Desarrollo de esquemas de evaluación;**
  - **Desarrollo de ICS-CERTs;**
  - **Apoyo al desarrollo de marcos regulatorios.**;
  - **Desarrollo de sistemas que incluyen ciberseguridad** desde el diseño;
  - **Desarrollo de una cultura de ciberseguridad** dentro de los pilares de la seguridad industrial tradicional.
  - **Enfoque y capacitación** de las personas a cargo de los sistemas de control en los sistemas de seguridad de las TIC y viceversa;
  - **Mejora del cumplimiento legislativo;**
  - **Difusión de productos y soluciones** en ciberseguridad industrial entre todos los interesados.

2.2. ¿Cómo ha sido la adaptación para las empresas y la sociedad en general con respecto a la ciberseguridad?

2.2.1. Austria

En el segundo trimestre de 2015, PwC y Strategy y jointly publicaron conjuntamente el estudio "Industria 4.0 - La industria de Austria en cambio". En este estudio, se cuestionaron 100 empresas de cinco industrias en toda Austria (proveedores automotrices, ingeniería eléctrica y electrónica, ingeniería mecánica y de plantas y la industria de procesos). Para una implementación exitosa y oportuna de los conceptos de la Industria 4.0, las compañías aún deben dominar numerosos desafíos. Para un tercio de los encuestados, la atención se centra en las altas inversiones y un cálculo de rentabilidad a menudo poco claro, así como los estándares y normas que faltan para las nuevas aplicaciones de la Industria 4.0. Muchas empresas aún no han elaborado planes de implementación concretos para soluciones de la Industria 4.0 o inversiones aprobadas porque las soluciones son nuevas para muchas empresas, requieren cambios considerables y el potencial es difícil de cuantificar. Existe una gran necesidad de mayor transparencia y de un intercambio de experiencias entre industrias. También debe promoverse la estandarización internacional en el área de aplicaciones de la Industria 4.0 y esta es la única forma de intensificar la cooperación entre empresas y aumentar la eficiencia en el futuro. Los principales desafíos son:

- **Cualificación inadecuada de los empleados;**
- **Protección de datos;**
- **Seguridad de datos.**

El cambio digital cambiará las demandas que se imponen a los empleados en todas las etapas de la cadena de valor, desde el desarrollo hasta la producción y las ventas, y la creciente digitalización hará que los procesos y los modelos comerciales sean más ágiles e impulsados por los datos. Esto exige habilidades y cualificaciones completamente nuevas de los empleados. La demanda de desarrolladores de software y analistas de datos en la industria también aumentará significativamente en los próximos cinco a diez años (Busch et al., 2015).

La adaptación de las empresas y la sociedad en general con respecto a la ciberseguridad ya está en progreso, pero se necesitan más adaptaciones y compromisos no solo de las autoridades públicas, sino también de las empresas individuales y de cada individuo que vive en esta sociedad. Diversas iniciativas, como la asociación Platform Industry 4.0 y la Comisión de Seguridad de la Información están ayudando a este respecto al proporcionar asesoramiento. A medida que las posibilidades digitales continúan evolucionando y cambiando, también existe la necesidad de un desarrollo continuo en términos de seguridad.

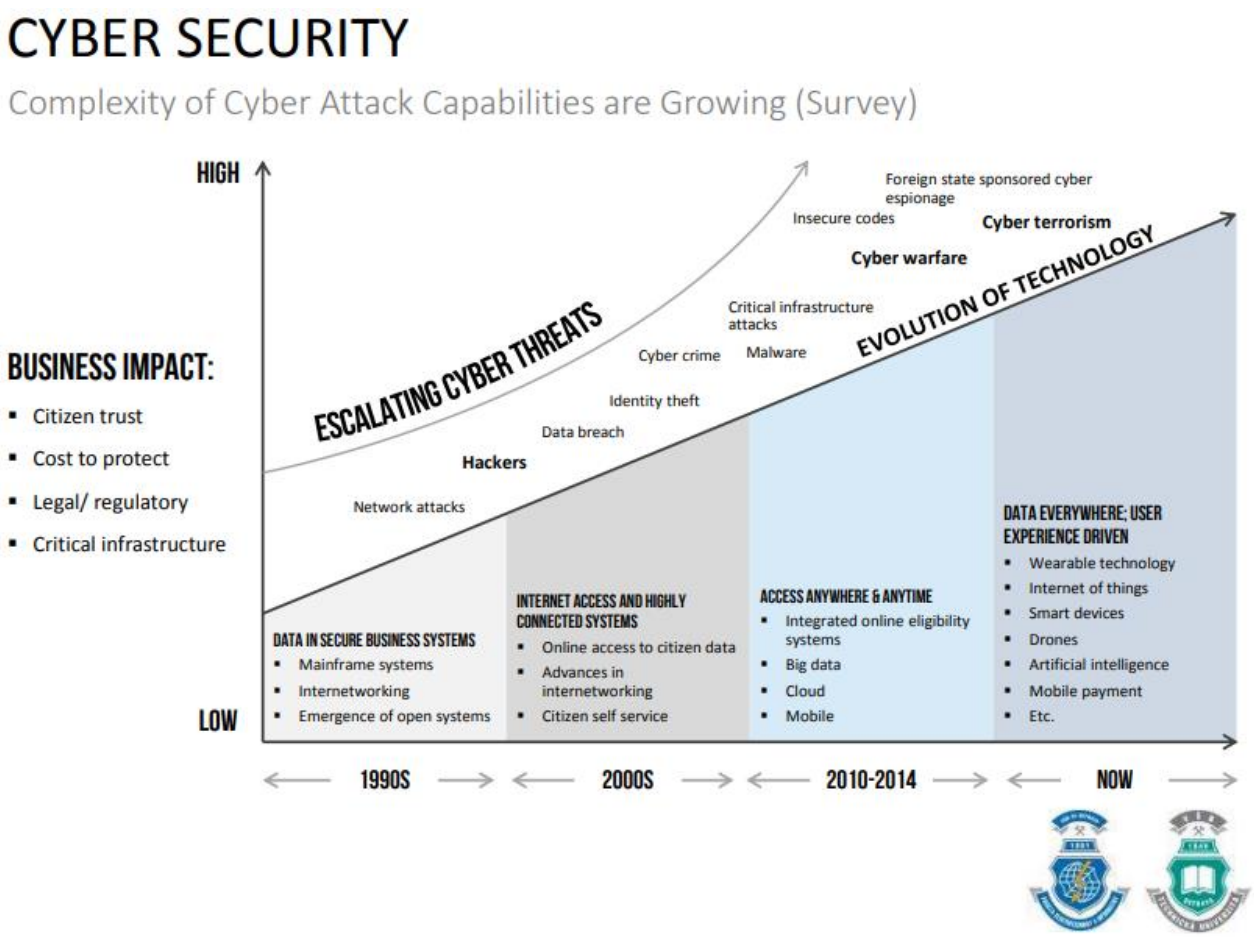
2.2.2. República Checa

Con respecto a la adaptación de las empresas y la sociedad en general en cuanto a la ciberseguridad, existen algunos efectos comerciales que afectan a las empresas, por ejemplo:

- **Confianza ciudadana;**
- **Coste para proteger;**
- **Impacto legal/regulatorio;**
- **Infraestructura crítica.**

La Facultad de Ingeniería Eléctrica e Informática de VŠB-TUO en la República Checa analizó las crecientes amenazas cibernéticas durante la evolución de la tecnología entre 1990-2018 y se descubrió que la complejidad de las capacidades de ataque cibernético está creciendo. En la siguiente figura podemos ver los resultados de estas amenazas.

Figura 2 - Amenazas en el ciberespacio



Fuente: (VŠB-TUO, n.d.)

Como podemos ver en la figura anterior, el número de problemas de seguridad cibernética está aumentando desde 1990. Con la evolución de la tecnología, las amenazas cibernéticas están aumentando y después de 2010-2014 las principales amenazas cibernéticas críticas son:

- **Malware;**
- **Ataques críticos de infraestructura;**
- **Guerra cibernética;**
- **Códigos inseguros;**
- **Terrorismo cibernético;**
- **Espionaje cibernético patrocinado por el estado extranjero.**

2.2.3. Portugal

La rápida transformación digital trae de golpe una nueva problemática relacionada con la ciberseguridad.

El Centro Nacional de Cibersegurança (CNCS) tiene como objetivo garantizar un ciberespacio nacional seguro y funciona en diferentes fases, especialmente la fase de reacción que se refiere a cuando algo sale mal y es la entidad formal responsable de la ciberseguridad nacional. Además, CNCS creará un instrumento llamado **"Modelos de Maturidade para a Cibersegurança"** que traerá un conjunto de medidas y controles para aplicar y definirá algunas prioridades para crecer en la madurez de la ciberseguridad. Este instrumento se dividirá en cuatro documentos: 1) cómo reaccionar ante incidentes; 2) cómo prevenir incidentes; 3) cómo detectar incidentes; y 4) gestión de la información de seguridad. Este instrumento estará disponible en 2019 y también incluirá algunas buenas prácticas que sin duda serán muy útiles.

El CNCS tiene un papel muy activo cuando se trata de este tema, en febrero de 2019 lanzó un curso en línea gratuito que tiene como objetivo aumentar el conocimiento y la alfabetización en el área de seguridad, abordando temas como la actualización de software, el uso de pen drives y contraseñas y su uso en contexto personal y profesional.

Además, el CNCS está trabajando con programas de cooperación nacionales e internacionales. En realidad, en esta área, Portugal tiene una de las redes de cooperación más grandes para reaccionar a los incidentes de ciberseguridad en Europa y este centro solo se creó en 2014.

La mayoría de los eventos de ciberseguridad provienen de:

- **Incidentes internos porque a veces los trabajadores tienen, sin ninguna mala intención, algún comportamiento o actitud que puede conducir a algunos incidentes.** Debido a esto, proporcionar actividades de capacitación a todos los trabajadores es crucial para evitar algunos de los incidentes que pueden ocurrir. Además, aunque las inversiones en capacitación son fundamentales, las infraestructuras digitales, como el software y el hardware, no pueden olvidarse porque dan como resultado una mayor seguridad del sistema informático;
- **Ataque de suplantación de identidad**. Los portugueses invierten poco en ciberseguridad y, por lo tanto, son más vulnerables a los ataques. Esto sucede porque la mayoría de las empresas todavía prefieren tratar las cosas internamente ya que

consideran que esta área aún no es una prioridad. Esto puede explicarse por el hecho de que la mayoría de las empresas portuguesas son PYMEs;

- **La tecnología obsoleta y la ciberseguridad** son dos aspectos que todo gerente considera que bloquean la progresión de sus negocios. Además, las organizaciones portuguesas confirman que la ciberseguridad está actuando como un freno a la productividad, ya que casi la mitad de los líderes tecnológicos y empresariales consideran que la ciberseguridad tiene un impacto negativo;
- **Los procedimientos de seguridad de autenticación son complejos o consumen más tiempo**, cuando realizan una tarea urgente o con una fecha límite particularmente ajustada, pueden sentirse alentados a tomar caminos incorrectos y seguir "atajos";
- **La falta de competencias y capacidades digitales sigue siendo un gran problema**, aunque hay más información e iniciativas en línea y fuera de línea llevadas a cabo por instituciones públicas y privadas que tienen como objetivo promover un comportamiento y una actitud más seguros. Sin embargo, especialmente la generación más joven se está volviendo más cómoda y tiene más conocimiento para lidiar con problemas de ciberseguridad.

Debido a esto, las empresas **deberían adoptar algunas estrategias de seguridad claras que brinden seguridad a los clientes** y deberían tener algunos planes de resolución cuando se trata de una crisis de ciberseguridad.

Para concluir, podemos decir que Portugal tiene algunas iniciativas relacionadas con la ciberseguridad llevadas a cabo en los últimos años y también hay algunas iniciativas que tienen como objetivo promover un comportamiento y una actitud mucho más seguros por parte de la sociedad en general. Sin embargo, aún queda mucho por hacer para tener un mejor entorno seguro tanto en las empresas como en la vida privada de los ciudadanos.

2.2.4. España

Los proyectos de ciberseguridad en España tienen como objetivo aumentar la seguridad de las aplicaciones, servicios e infraestructuras actuales y apoyar la creación de mercados líderes

en Europa, siempre con un enfoque de usuario final e incluyendo a todos los organismos competentes en materia de cumplimiento, operadores de infraestructura crítica, proveedores de servicios de TIC, distribuidores de TIC, actores del mercado y ciudadanos. Todo esto requiere fortalecer las capacidades para enfrentar las amenazas del ciberespacio. Por lo tanto, sería conveniente:

- **Reforzar la capacidad de investigar y enjuiciar el delito cibernético**, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio;
- **Promover la ciberseguridad de ciudadanos y empresas;**
- **Fomentar la industria española de ciberseguridad,** asegurando la generación y retención de talento personal, con el fin de fortalecer la autonomía digital;
- **Contribuir y promover un ciberespacio abierto, plural, seguro y confiable,** apoyando los intereses nacionales;
- **Desarrollar una cultura de ciberseguridad.**

3. Internet safety and Industry 4.0: in companies

Se espera que las tecnologías de la Industria 4.0 impulsen una mayor evolución en la estructura tradicional de la cadena de suministro lineal al introducir plataformas y dispositivos inteligentes y conectados en todo el ecosistema, lo que da como resultado una red de suministro digital (DSN) en la cadena de valor para informarse mutuamente. El resultado puede ser una mejor gestión y flujo de materiales y bienes, un uso más eficiente de los recursos y suministros que satisfaga más adecuadamente las necesidades del cliente. Si bien conlleva muchos beneficios, la creciente interconexión del DSN también conlleva debilidades cibernéticas que deben planificarse adecuadamente y contabilizarse en cada etapa, desde el diseño hasta la operación, para evitar riesgos significativos.

Pero una red ágil y receptiva de esta naturaleza solo es posible mediante el intercambio abierto de datos de todos los participantes en la red de suministro, lo que crea problemas importantes y puede generar algunas dificultades entre permitir la transparencia de algunos datos y mantener la información.

Por lo tanto, es posible que las organizaciones deseen considerar formas de **proteger esa información para evitar que usuarios no autorizados** accedan a ella a través de la red, especialmente cuando se trata de procesos de apoyo como el intercambio de información y el acceso al sistema.

El principal factor importante a tener cuidado es la confianza. Es posible que las organizaciones necesiten s**eguir evolucionando su gestión de riesgos para preservar la integridad** y permanecer seguros al realizar transacciones de información o bienes, así como fortalecer sus capacidades de monitoreo y operaciones de ciberseguridad para permanecer vigilantes y proteger procesos que no pueden validarse.

3.1. ¿Qué accidentes relacionados con la seguridad en Internet se resolvieron en su país en los últimos años en las empresas?

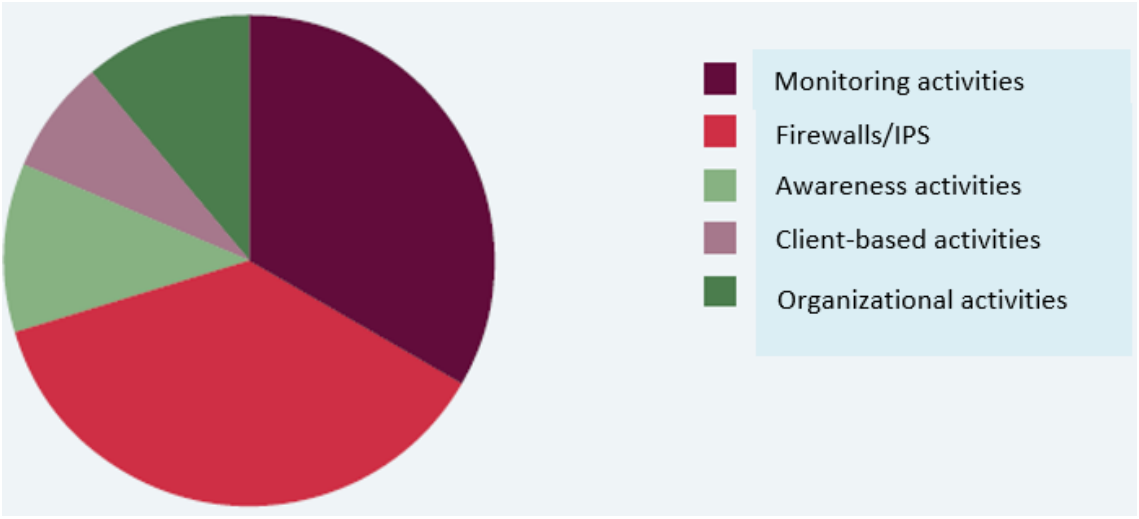
3.1.1. Austria

En Austria hay algunos ejemplos de accidentes relacionados con la seguridad en Internet, como, por ejemplo, Amenazas Persistentes Avanzadas (APT). En octubre de 2018, Austria se convirtió en víctima de tal ataque, con el objetivo de poner en peligro la seguridad de los sistemas informáticos de las autoridades e instituciones públicas y robar datos a gran escala. Los atacantes utilizaron una variedad de canales para intentar infectar a las víctimas con *malware* con el fin de comprometer los datos del usuario, con el objetivo final de infiltrarse en las redes de los ordenadores y robar datos confidenciales.

Las precauciones tomadas por las instituciones atacadas y la buena cooperación entre GovCERT y el Centro de Seguridad Cibernética (CSC) permitieron defenderse de los ataques a todos los afectados y evitar la salida de datos. El hecho de que los efectos se hayan mantenido mínimos a pesar del esfuerzo de los atacantes es una señal más de la efectividad y la importancia de la cooperación continua entre todos los organismos relevantes a nivel nacional (Cyber Sicherheit Steuerungsgruppe, 2019).

En la siguiente figura, tenemos una visión general de las medidas de seguridad introducidas.

Figura 3 - Medidas tomadas (2018)



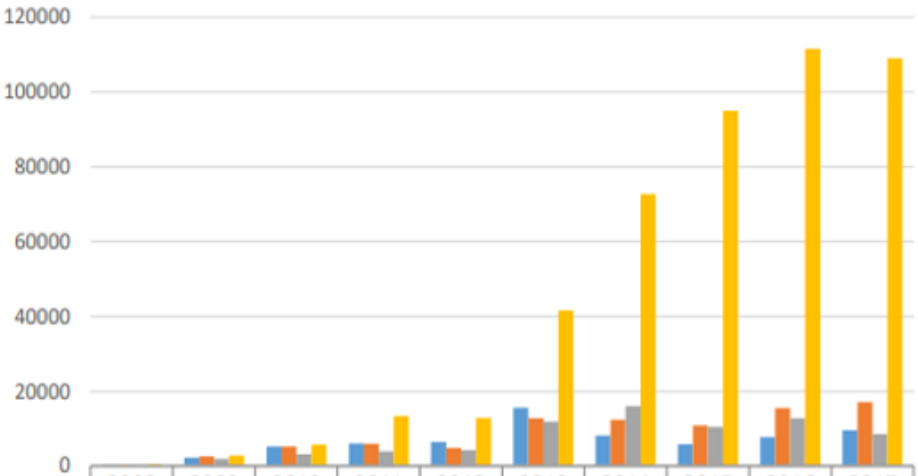
Fuente: (Cyber Sicherheit Steuerungsgruppe, 2019)

Si bien el progreso técnico en las áreas de cortafuegos/SPI y protección de puntos finales indudablemente ha llevado a mejoras en las medidas de defensa, la tendencia del año pasado también continúa aquí: en lugar de centrarse exclusivamente en el aislamiento, cada vez más

organizaciones tienden a **monitorear medidas para detectar atacantes en sus propias redes.** Esto también incluye la **búsqueda activa de amenazas actuales para la organización respectiva** y, en un segundo paso, la verificación selectiva de los sistemas para detectar infecciones. Además, se tomaron medidas preparatorias en muchos lugares para poder analizar incidentes de seguridad utilizando métodos forenses (Cyber Sicherheit Steuerungsgruppe, 2019).

Figura 4 - 29

CERT.at annual statistics



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
False alarms	187	2227	5209	6006	6460	15592	8178	5740	7701	9537
Relevant reports	210	2593	5190	5938	4878	12755	12346	10884	15499	17055
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809	8556
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550	109003

Fuente: (Nic.at GmbH, 2018)

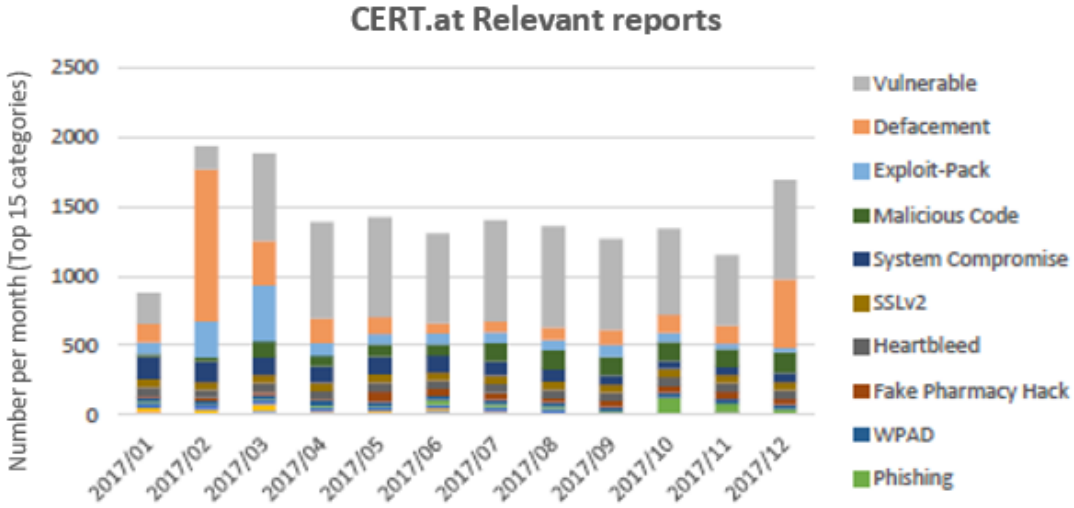
Desde 2008, el equipo Computer Emergency Response Team (CERT) .at ha liderado las estadísticas anuales generales. Estas incluyen el número de informes relevantes, incidentes e investigaciones, así como falsas alarmas. Desde 2008 hasta 2017, CERT.at está trabajando para mejorar continuamente la ciberseguridad en Austria. En la figura 4, podemos ver la cantidad de informes, incidentes e investigaciones a lo largo del tiempo y podemos confirmar que la cantidad de informes relevantes es significativamente mayor que el resto de las categorías. La explicación para cada una de las siguientes categorías se describe a continuación.

Los "informes relevantes" se refieren a los informes entrantes al CERT. No todos describen una situación que el CERT.at clasifique como un incidente relevante y requiere tratamiento activo.

Los "incidentes" son aquellos casos que en realidad representan un riesgo de seguridad. En estos casos, CERT.at se activa e informa a las empresas, organizaciones o usuarios privados afectados, por ejemplo, sobre las amenazas de seguridad de TI y, en casos especiales, los ayuda a resolver problemas.

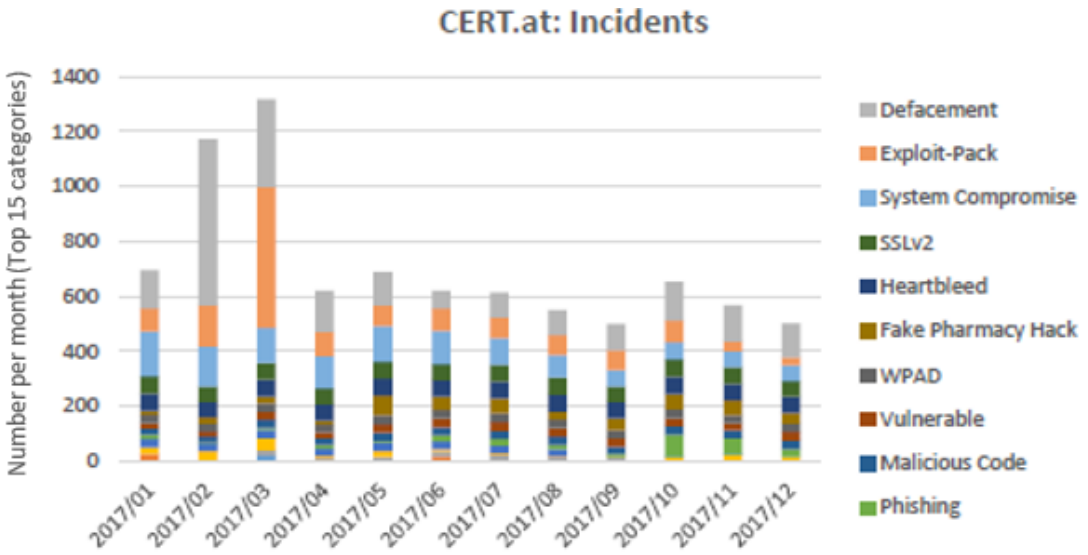
En el sistema de tickets CERT.at, contactar a las compañías, organizaciones o usuarios privados afectados se conoce como "Investigación". Una investigación suele ser un correo electrónico al operador de red, proveedor de alojamiento web o propietario del dominio. En las figuras 5, 6 y 7 tenemos una descripción general de los incidentes más comunes que ocurrieron en 2017 por categoría.

Figura 5 - Clasificación de informes relevantes por tipos de amenaza a lo largo del tiempo (2017)



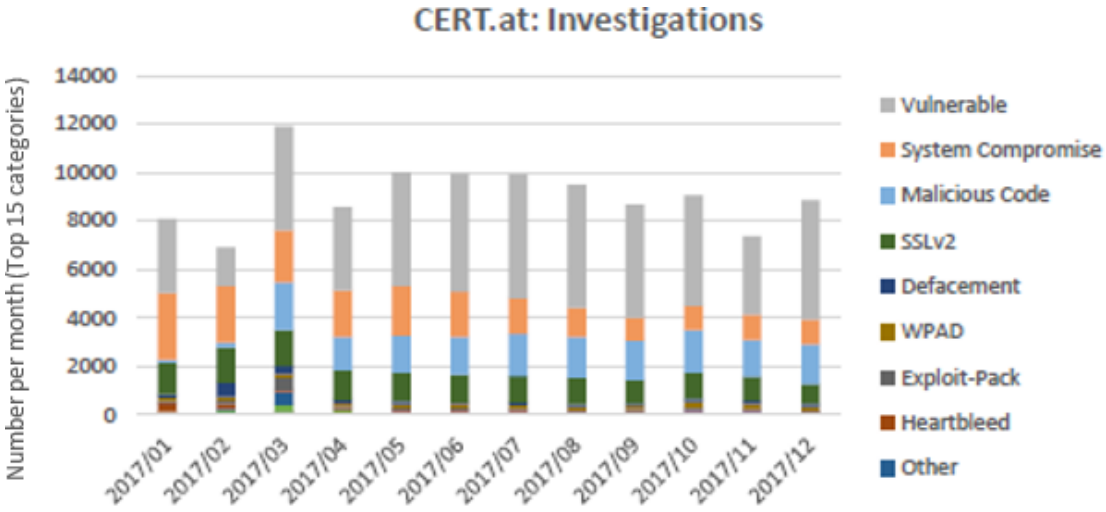
Fuente: (Nic.at GmbH, 2018)

Figura 6 - Clasificación de incidentes de acuerdo con los tipos de amenazas a lo largo del tiempo (2017)



Fuente: (Nic.at GmbH, 2018)

Figura 7 - Clasificación de las las investigaciones llevadas a cabo por CERT.at de acuerdo con las formas de amenaza a lo largo del tiempo (2017)



Fuente: (Nic.at GmbH, 2018)

3.1.2. República Checa

A partir del análisis nacional de casos de delitos en Internet en la República Checa, se reveló que las manifestaciones más destacadas de los delitos informáticos incluyen:

- **Estafa y malversación de fondos;**
- **Falsificación;**

- **Difamación;**
- **Venganza electrónica;**
- **Engaños;**
- **Warez;**
- **Penetraciones del sistema;**
- **Robo de ordenadores de bancos de (suplantación de identidad, pharming, IP spoofing).**

Los ciberdelincuentes han cambiado nuevamente y sus métodos son más sofisticados que antes y muchas empresas e instituciones no están preparadas para los actuales ataques electrónicos modernos. La Policía de la República Checa ha estado monitoreando el desarrollo de crímenes cometidos en el ciberespacio (principalmente dentro de Internet) desde 2011. Los casos de cibercrimen han aumentado constantemente desde entonces (de aproximadamente 1500 crímenes en 2011 a más de 5650 crímenes en 2017) el crecimiento se ha visto ralentizado en los últimos años. Los incidentes de CRIS.CZ en 2017 muestran que las mayores amenazas son:

- **Suplantación de identidad;**
- ***Malware*;**
- ***Spam*;**
- **Troyano.**

El ataque más común es el phishing mediante la obtención de información confidencial, como números de tarjetas de crédito o quizás contraseñas de cuentas. Sin embargo, los correos electrónicos falsos de los directores de la compañía también son comunes con el comando de transferir una cierta cantidad de dinero a una cuenta determinada.

3.1.3. Portugal

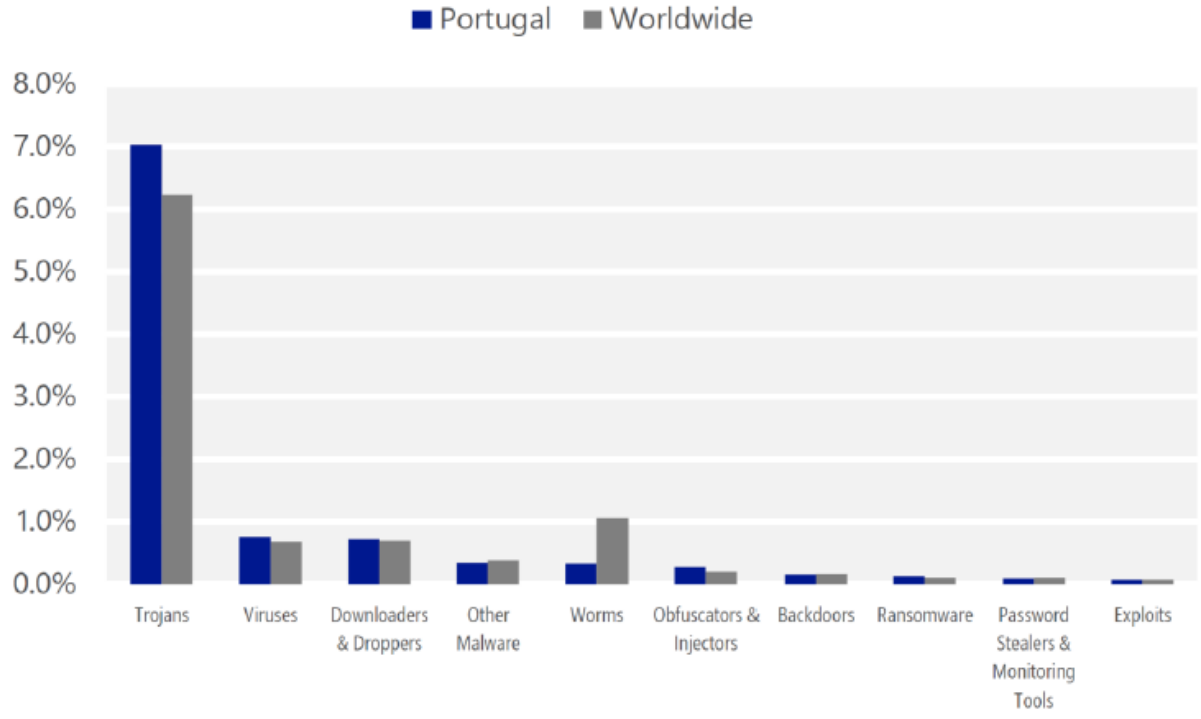
In Portugal, the most common attacks are:

- **Phishing attacks** that are, generally, followed by SPAM messages send to multiple users. While there may be phishing types that request the data directly in response to

the email, they are most often articulated with a website where you fill in your data. In 2018 Portugal was the second country in the world with more phishing attacks according to the study "Spam and Phishing in 2018" carried out by Kaspersky Lab about online security;

- **Violaciones de ciberseguridad (datos robados);**
- Los **ataques de "ransomware"** disminuyeron en Portugal en 2018 y el phishing sigue siendo el método de ataque favorito. Además, Portugal todavía está un poco por debajo del promedio internacional en la detección de violaciones de seguridad cibernética, a excepción de la identificación de episodios de minería de criptomonedas .;
- **Malware y troyanos.** Según un informe realizado por Gabinete de Estratégia e Estudos, Portugal es uno de los países que tiene una de las tasas de incidentes de malware más altas y este es el software malicioso más común en Portugal junto con los troyanos (ver figura 8).

Figura 8 - Ratio de incidencia de software malicioso (march 2017)



Fuente: Microsoft (2018)

- **La inteligencia de amenazas en la nube (amenaza "en la nube")** es una de las amenazas más recientes para la seguridad de la información en este momento porque el uso de la nube es utilizado actualmente por la mayoría de las empresas y, con eso, lo convierten en un objetivo cada vez mayor para los ataques. Los piratas informáticos ingresan en la nube de las organizaciones a través de credenciales de acceso robadas a un usuario, en gran parte debido al uso de contraseñas débiles seguidas de ataques de phishing dirigidos y violaciones de servicios de terceros. Según Microsoft (2017), los ataques a las cuentas de usuarios de la nube aumentaron un 300% en el primer trimestre de 2017 en comparación con el primer trimestre de 2016.

Según los resultados del mismo estudio, Portugal es el octavo país con la mayor puntución de vulnerabilidad al delito cibernético y uno de los países con mayor número de víctimas del delito cibernético en la UE (3ª posición).

Figura 9 - Puntuación de vulnerabildiad al cibercrimen

EU COUNTRY	CYBERCRIME VULNERABILITY SCORE				
1. MALTA (MOST VULNERABLE)	42%	11. SLOVENIA	38%	21. SWEDEN	32%
2. GREECE	41%	12. CROATIA	37%	22. ITALY	31%
3. ROMANIA	41%	13. DENMARK	36%	23. FRANCE	31%
4. SLOVAKIA	40%	14. LATVIA	35%	24. UK	31%
5. SPAIN	40%	15. CZECH REP	35%	25. NETHERLANDS	30%
6. LITHUANIA	39%	16. POLAND	34%	26. GERMANY	30%
7. CYPRUS	39%	17. IRELAND	33%	27. ESTONIA	30%
8. PORTUGAL	39%	18. LUXEMBOURG	32%	28. FINLAND (LEAST VULNERABLE)	29%
9. HUNGARY	39%	19. AUSTRIA	32%		
10. BULGARIA	38%	20. BELGIUM	32%		

Fuente: Website Builder Expert (2017)

Figura 10 - Clasificación de victimización del cibercrimen

Biggest Cybercrime victims in the EU	% OF POPULATION WHO HAVE EXPERIENCED CYBERCRIME	ANNUAL AVERAGE MALWARE ENCOUNTER RATE	CYBERCRIME VICTIMHOOD RATING
1. ROMANIA	18%	28%	23%
2. NETHERLANDS	27%	14%	21%
3. PORTUGAL	15%	24%	20%
4. POLAND	16%	23%	20%
5. ITALY	17%	21%	19%

Fuente: Website Builder Expert (2017)

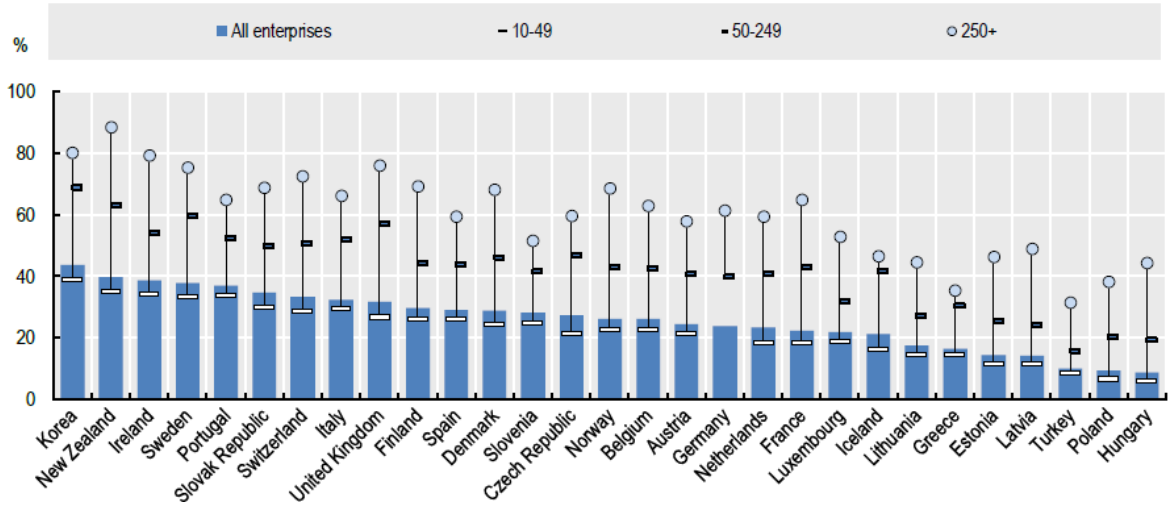
Sin embargo, es importante afirmar que Portugal tiene un alto porcentaje de ordenadores con software de seguridad habilitado, pero sigue siendo uno de los países más vulnerables a los delitos de ciberseguridad.

En cuanto a la dimensión de las empresas, las más afectadas son aquellas con entre 50 y 249 trabajadores (47,1%), seguidas por las empresas con más de 250 trabajadores (42,6%) mientras que las empresas entre 10 y 49 trabajadores son las que están menos expuestos a este tipo de incidentes (OCDE, 2017).

Cuando se trata de empresas que tienen una política formal para gestionar sus riesgos de privacidad digital, Portugal es uno de los países que tiene más políticas implementadas en sus empresas.

Figura 11 - Empresas que tienen una política formal para gestionar los riesgos de privacidad digital. (2015)

(% de todas las compañías)



Fuente: OECD (2017)

En conclusión, el riesgo de incidentes de ciberseguridad en Portugal es mucho mayor que el del resto de las empresas de la UE28.

Cuando se trata de la seguridad de los datos, las principales preocupaciones de las empresas portuguesas son:

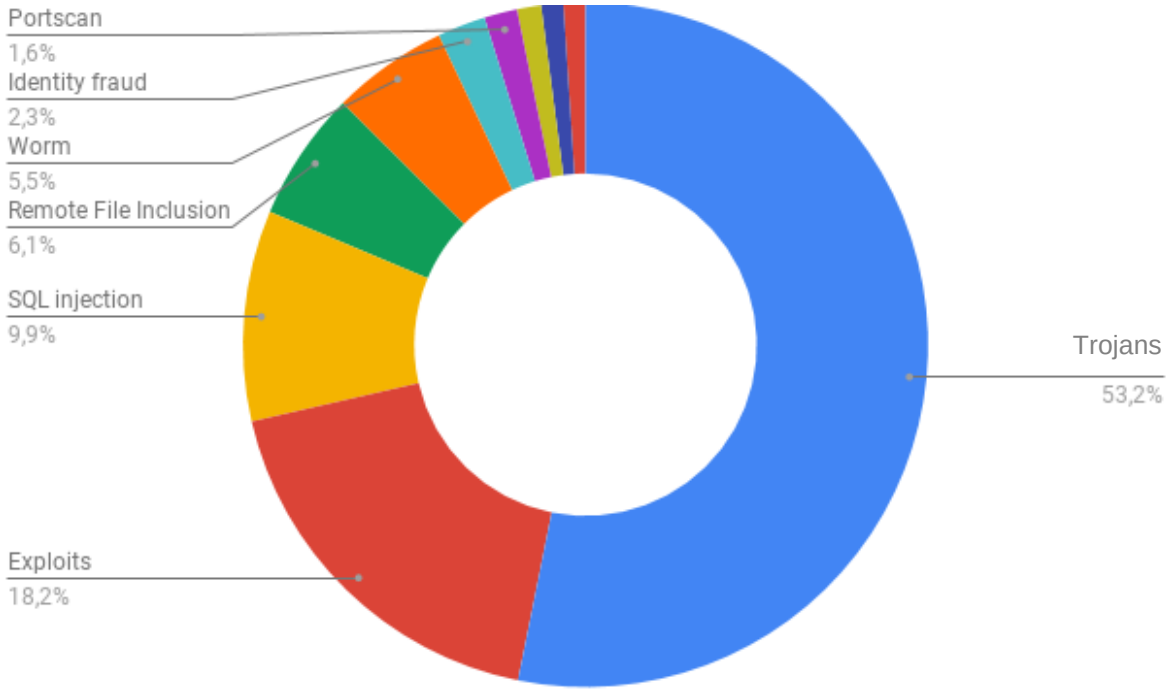
- **Gestión interna de datos** (61%), como los riesgos inherentes a la responsabilidad de pérdida de datos (59%),
- **Infracciones o fallos de ciberseguridad** (43%)
- **Uso indebido de datos durante el intercambio de datos con socios** (43%).

3.1.4. España

Como podemos ver en la figura anterior, los ataques más comunes en España son:

- Troyanos;
- Explotaciones e inyección SQL.

Figura 12 - Incidentes más comunes



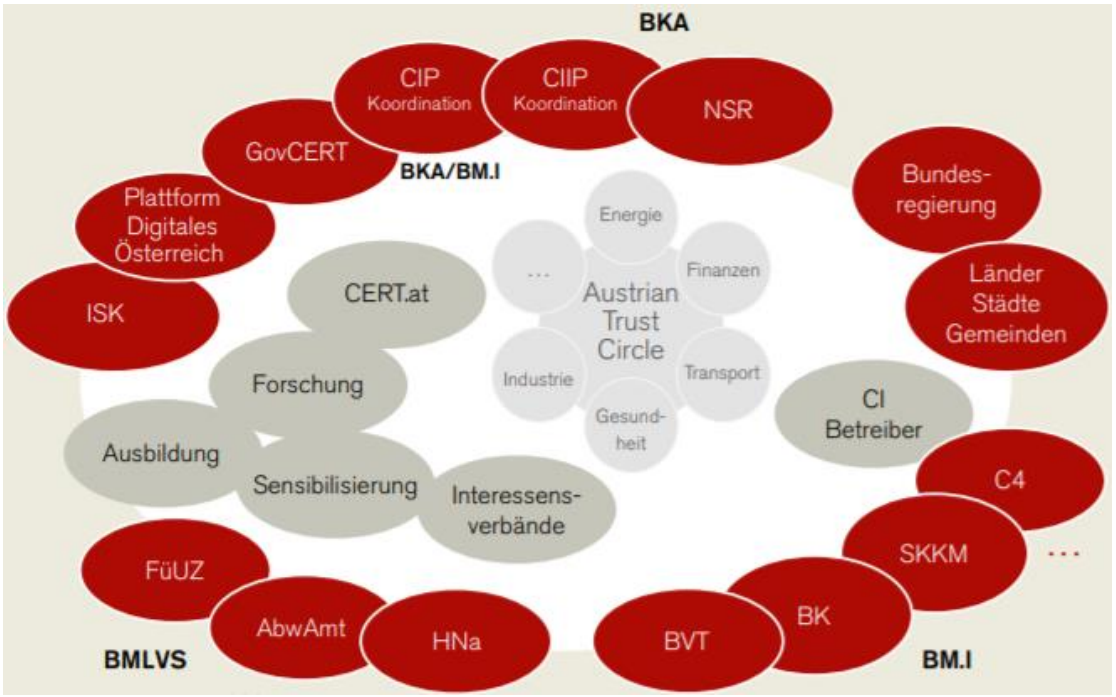
Fuente: Author's own elaboration from (ccn-cert.cni, n.d.)

3.2. ¿Existen en su país equipos para monitorear la seguridad en Internet y la ciberseguridad con respecto a las empresas?

3.2.1. Austria

En el área del ciberespacio hay muchas estructuras y partes interesadas austriacas que trabajan con la ciberseguridad de manera muy distribuida. Varias organizaciones que trabajan exclusivamente en ciberseguridad ya están jugando un papel importante en Austria, como los CERT establecidos.

Figura 13 - Partes interesadas en Austria en casos de ciberataque



Fuente: (Bundeskanzleramt, Digitales Österreich, 2012)

CERT.at es el Equipo Nacional de Respuesta a Emergencias Informáticas de Austria, establecido en 2008 junto con GovCERT Austria por la Cancillería Federal (BKA) en cooperación con nic.at, el registro de dominio austríaco, como un proyecto en nic.at. Como tal, CERT.at es el contacto para la seguridad de TI en el entorno nacional y es responsable de todos los casos que no están cubiertos por un CERT más específico.

CERT.at conecta en red a otros equipos de respuesta a emergencias informáticas y equipos de respuesta a incidentes de seguridad informática de las áreas de infraestructura crítica y tecnología de la información y la comunicación (TIC) y ofrece advertencias, sugerencias sobre casos concretos y soluciones para empresas y particulares.

GovCERT Austria es el Equipo de Respuesta de Emergencia Informática del Gobierno para el sector de la administración pública en Austria. Por lo tanto, sirve como el principal punto de contacto a nivel nacional para los órganos individuales de la administración pública en caso de un ciberataque.

A nivel internacional, GovCERT Austria actúa como el punto de contacto austriaco para gobiernos extranjeros y organizaciones internacionales en temas de seguridad de las TIC.

Intercambia información y advertencias con ellos y, si es necesario, los reenvía a las partes interesadas nacionales (Nic.at GmbH, 2018).

CERT.at y GovCERT son los soportes, dentro del alcance de sus posibilidades y especificaciones, en incidentes de seguridad. Si bien este soporte se limita, en la mayoría de los casos, a la provisión de información como notas técnicas o referencias a proveedores comerciales para proveedores de servicios de Internet o propietarios de dominios, CERT.at y GovCERT actúan como un punto de coordinación e interfaz entre las partes afectadas y otros actores relevantes a nivel nacional e internacional en caso de incidentes mayores. También proporciona instrucciones para la acción y comparte información sobre cómo eliminar las amenazas (Nic.at GmbH, 2018).

CERT.at no solo debe garantizar la seguridad en Internet en Austria, sino que también debe proteger la seguridad de los propios sistemas de TI y la infraestructura es un factor decisivo. Una certificación de acuerdo con ISO 27 001/2017 es la prueba de que la seguridad de TI en una empresa se trata de manera integral y, además del examen de la seguridad de los sistemas técnicos y la seguridad de la infraestructura física, incluidos los aspectos organizativos. La certificación ISO 27 001 es un sello de calidad para el mundo exterior y, por otro lado, también un incentivo continuo para garantizar la propia seguridad interna. Las auditorías anuales en CERT.at aseguran que este estándar se mantenga (Nic.at GmbH, 2018).

Los CERT más importantes en Austria son: A1-CERT; ACOnet-CERT; Austrian Energy CERT; BRZ-CERT; CERT.at; CERT-Verbund Österreich; GovCERT Austria; MilCERT; Raiffeisen Informatik CERT; SCERT; SV-CERT; TSA CERT; WienCERT; WILICERT.

3.2.2. República Checa

Hay muchas organizaciones en la República Checa que participan activamente en la protección del ciberespacio. Los ejemplos incluyen CERT o Equipo de respuesta a incidentes de seguridad informática (CSIRT.CZ). Los CERT se encuentran en las organizaciones de seguridad informática predominantes y en varios sectores mundiales de gobierno, comercio y académico. Aborda cuestiones técnicas de ciberseguridad, incluida la resolución de incidentes de seguridad de sujetos que administran importantes sistemas de comunicaciones e información para el gobierno, el análisis de malware, la recopilación y evaluación de

información sobre ataques cibernéticos y amenazas, etc. CERT.CZ realiza tareas tales como garantizar la prevención de amenazas cibernéticas y ataques contra operadores de infraestructura de información cruciales y autoridades públicas y garantizar y coordinar soluciones de incidentes de ciberseguridad de operadores de infraestructura de información cruciales y autoridades públicas.

Los CSIRT suelen ser servicios responsables de recibir, revisar y responder a informes y actividades de incidentes de seguridad informática. Sus servicios generalmente se realizan para un componente definido que podría variar de una corporación a un cliente que paga.

En la República Checa, el Instituto Checo de Informática, Robótica y Cibernética (IDSA) se creó para proporcionar un entorno unificado para compartir datos entre usuarios en diferentes entornos industriales y de fabricación. El objetivo de IDSA es crear un ecosistema para compartir datos de forma segura que se base en un estándar unificado de intercambio de datos entre socios comerciales internacionales.

3.2.3. Portugal

En Portugal hay empresas privadas y un CNCS que ayudan a las empresas portuguesas con problemas de ciberseguridad con algunos servicios/soluciones para evaluar y tener un comportamiento y actitudes más responsables en línea.

Cuando se trata de compañías privadas, existen algunos servicios relacionados con la protección en línea que son proporcionados principalmente por compañías de seguros y de seguridad. Algunas de estas soluciones incluyen servicios que analizan todo el ciclo de vida de la ciberseguridad. En la siguiente figura, podemos ver un ejemplo de un servicio proporcionado por un grupo tecnológico.

El servicio se divide en cinco etapas: 1) identificar; 2) proteger; 3) detectar; 4) respuesta; y 5) recuperarse.

Figura 14 - Ciberseguridad servicios/soluciones

IDENTIFY

Fuente: Gmv (n.d.)

En Portugal también existe CERT.PT, que es una parte integral del CNCS que coordina la respuesta a incidentes que involucran a entidades estatales, operadores de servicios esenciales, operadores de infraestructuras críticas y proveedores de servicios digitales. A través de este servicio, CNCS coordina la respuesta a incidentes de seguridad cibernética que involucran entidades estatales, operadores de servicios esenciales y proveedores de servicios digitales, operadores de infraestructuras nacionales críticas y otro equipo nacional de respuesta a incidentes de seguridad informática.

La complejidad y la transnacionalidad de una gran cantidad de incidentes de ciberseguridad requieren una visión agregada y una acción coordinada entre las diversas entidades involucradas.

Además, las empresas de seguridad privada en Portugal son más activas cuando se trata de la presentación de servicios relacionados con la seguridad digital y los servicios de seguridad gestionados en el mercado. Sin embargo, la mayoría de las organizaciones aún no enfrentan la protección y la seguridad como parte integral de su estrategia.

3.2.4. España

En 2018, se publicaron dos nuevas instrucciones técnicas de seguridad en España:

- Resolución del 27 de marzo de 2018, del Secretario de Estado para el Servicio Civil, por la que se aprueba la Instrucción Técnica sobre Auditorías de Seguridad para los sistemas de seguridad de la información;
- Resolución del 13 de abril de 2018, de la Secretaría de Estado de Función Pública, que aprueba la Instrucción Técnica sobre Seguridad para la Notificación de Incidentes de Seguridad.

Ambos se suman al ITS de acuerdo con el Marco de Seguridad Nacional (ENS) y el Informe de Estado de Seguridad previamente publicado. Por otro lado, el proceso de transposición se está completando para la Directiva (UE) 2016/1148, del 6 de julio, la Directiva NIS, que también afectará al sector público y que, entre otras cuestiones:

- Identificará los operadores de servicios esenciales.
- Las medidas de seguridad a aplicar.
- Las autoridades competentes.
- Identificará los CSIRT de referencia.
- Asignará al CCN-CERT la coordinación y la respuesta técnica en casos particularmente severos.

Además, y como resultado de la plena aplicación del Reglamento (UE) 2016/679, del 27 de abril, sobre el procesamiento y la libre circulación de datos personales (GDPR), se ha elaborado un nuevo proyecto de Ley Orgánica de Protección de Datos que, derogando la ley actual , regulará cualquier problema que el Reglamento general de protección de datos deje a la Comisión.

Ccn-cert que asiste a las diferentes actividades del centro nacional de criptología ha desarrollado:

- ATHENEA es el nuevo instrumento de capacitación en desafíos de ciberseguridad que tiene como objetivo crear conciencia sobre la importancia de este campo.

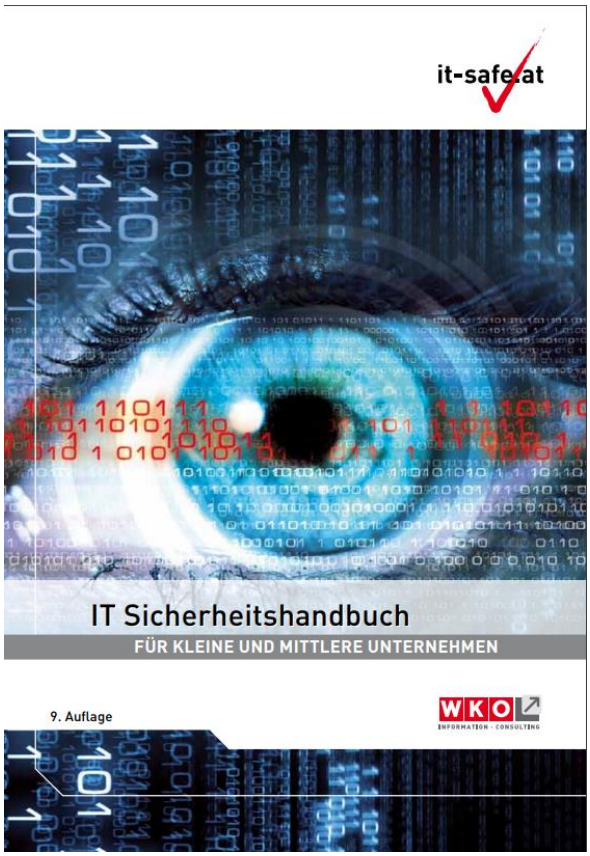
- GLORIA es una forma de plataforma y envejecimiento de incidentes y amenazas de seguridad cibernética, que también ha sido interoperable con las herramientas Carmen, Lucía y Reyes para facilitar la detección, el análisis y el intercambio de incidentes.
- SAT_ICS- La función principal del Sistema de Alerta Temprana para Sistemas de Control Industrial es la detección temprana de incidentes de seguridad. También permite el acceso a un mayor número de reglas de detección y la correlación de eventos, favoreciendo el soporte para la resolución de incidentes.

3.3. ¿Qué hacen esos equipos cuando enfrentan un incidente de ciberseguridad con respecto a las empresas?

3.3.1. Austria

En el caso de la seguridad de TI para las PYME, pueden usar la guía en línea segura para evaluar la seguridad de su propia infraestructura de TI. El Manual de seguridad de TI para pymes proporciona información práctica sobre posibles peligros y las medidas técnicas adecuadas para contrarrestarlos. En este manual podemos encontrar los siguientes contenidos: gestión de riesgos; cumplimiento de requisitos legales; Consideraciones estratégicas de TI; medidas de personal; seguridad informática y protección antivirus; Seguridad de la red; respaldo de datos y preparación para emergencias; medidas de construcción e infraestructura; Grupo de expertos en seguridad de TI; y, policía - prevención del delito.

Figura 15 - Manual it-safe-at



Fuente: (WKO Bundessparte Information und Consulting, 2019)

En el caso de la lista de verificación de EPU para compañías unipersonales, se puede determinar en solo unos minutos si hay y dónde podría haber problemas de seguridad en el área de TI. En una emergencia (por ejemplo, un ataque cibernético o el cifrado de sus datos por un troyano para chantajear), la línea directa de seguridad cibernética al 0800 888 133 puede proporcionar asistencia gratuita durante todo el día.

La línea directa de ciberseguridad es un sistema de tres pasos:

1) El centro de llamadas ofrece 24 horas al día, 7 días a la semana al 0800 888 133 (sin cargo para los miembros) información telefónica inicial y asistencia de emergencia;

2) El centro de llamadas ofrece medidas iniciales simples, etc., pero no diagnósticos técnicos remotos, ni asistencia legal o preguntas sobre prevención, coordenadas (sin cargo para los miembros) pero con gusto, si es necesario y deseado, el contacto con una empresa del Grupo de Expertos UBIT IT- Seguridad especializada en seguridad informática y cibercrimen desde su proximidad. Es aconsejable aprovechar esta consulta inicial gratuita con la compañía de seguridad de TI;

3) La empresa de seguridad de TI se pone en contacto con los dañados y realiza una primera reunión gratuita sobre la base de los datos generados por el centro de llamadas. Aunque los diagnósticos remotos nunca pueden dar una imagen completa, estos especialistas pueden evaluar mejor su situación y, si es necesario, proporcionar información sobre medidas inmediatas más concretas y medidas de afrontamiento para el establecimiento de operaciones normales. También ayuda a determinar si, y de qué forma, la empresa de seguridad de TI puede ayudar con una posible implementación en el sitio, que va más allá de la consulta inicial y está sujeta a un cargo. Cualquier otra tarea debe acordarse directamente con la empresa de seguridad de TI; los costos (tarifa por hora, etc.) para otras actividades también deben acordarse directamente con la compañía de seguridad de TI.

3.3.2. República Checa

Hay muchas organizaciones en la República Checa que participan activamente en la protección del ciberespacio. Los ejemplos incluyen CERT o CSIRT.CZ.

Los CERT se encuentran en muchas organizaciones de seguridad informática y en varios sectores globales de gobierno, comercio y académicos. Aborda cuestiones técnicas de ciberseguridad, incluida la resolución de incidentes de seguridad de sujetos que administran importantes sistemas de comunicaciones e información para el gobierno, el análisis de malware, la recopilación y evaluación de información sobre ataques cibernéticos y amenazas, etc. CERT.CZ realiza tareas tales como garantizar la prevención de amenazas cibernéticas y ataques contra operadores de infraestructura de información cruciales y autoridades públicas y garantizar y coordinar soluciones de incidentes de ciberseguridad de operadores de infraestructura de información cruciales y autoridades públicas.

Los CSIRT suelen ser servicios responsables de recibir, revisar y responder a informes y actividades de incidentes de seguridad informática. Sus servicios generalmente se realizan para un componente definido que podría variar de una corporación a un cliente que paga.
En la República Checa, IDSA se creó para proporcionar un entorno unificado para compartir datos entre usuarios en diferentes entornos industriales y de fabricación. El objetivo principal de este instituto es crear un ecosistema para el intercambio seguro de datos que se base en un estándar unificado de intercambio de datos entre socios comerciales internacionales.

3.3.3. Portugal

En el caso de Portugal, CNCS actúa como coordinador operativo y autoridad nacional especializada en ciberseguridad junto con entidades de los operadores de Infraestructuras Críticas Nacionales. En otras palabras, CNCS promueve el uso del ciberespacio de manera gratuita, confiable y segura mediante la mejora continua de la ciberseguridad nacional y la cooperación internacional. El papel de esta institución es proporcionar información y crear conciencia no solo de las entidades públicas y las infraestructuras críticas, sino también de las empresas y la sociedad civil. Por otro lado, es importante que el país esté equipado con recursos cualificados para lidiar con recursos humanos cualificados para enfrentar los complejos desafíos de la seguridad del ciberespacio.
Esta institución tiene, por lo tanto, un papel crucial en este campo en Portugal y es responsable de organizar y dar diferentes tipos de herramientas para difundir una cultura de seguridad que promueva todo el conocimiento, la conciencia y la confianza necesarios para usar los sistemas de información, reduciendo la exposición a riesgos del ciberespacio.
La misión de CNCS es implementar las medidas e instrumentos necesarios para anticipar, detectar, reaccionar y recuperar situaciones que, debido a la inminencia o ocurrencia de incidentes o ataques cibernéticos, pueden poner en peligro el funcionamiento de las agencias estatales, las infraestructuras críticas y los intereses nacionales.
Los equipos que trabajan en estas organizaciones organizan:

- **Eventos** como C-DAYS que es un evento de referencia nacional que enfoca uno de los grandes temas relacionados con la seguridad de la información y el ciberespacio. Este

evento ocurre cada año y tiene múltiples actores (industria, sociedad, gobierno, industria, académico, ...) involucrados;

- **Sesiones de sensibilización en múltiples temas** sobre ciberseguridad que se pueden ver en el sitio web del CNCS;
- **Seminars** designated by "Cibertemas" related to cybersecurity and also promotes project promotion, debate and the share of ideas.
- **Programa de concienciación y capacitación** en ciberseguridad en diferentes partes del país, de norte a sur, pasando por la isla contando con el apoyo de socios;
- La posibilidad de **notificar y obtener ayuda ante la eventual presencia de algún incidente;**
- **Cursos generales** de ciberseguridad que dura dos días. La mayoría de estos tipos de eventos son gratuitos pero necesitan registrarse.

Como se mencionó anteriormente, CERT.PT es una parte integral del CNCS que coordina la respuesta a incidentes que involucran entidades estatales, operadores de servicios esenciales, operadores de infraestructuras críticas y proveedores de servicios digitales. La coordinación de la respuesta a incidentes incluye:

- La revisión de informes de incidentes, su análisis técnico y forense;
- La articulación con las entidades nacionales e internacionales involucradas;
- La coordinación de la respuesta a incidentes puede ser iniciada por el CNCS, por ejemplo, en una situación de incidentes a gran escala o puede ser solicitada por canales designados para ese propósito.

En caso de necesidad, el CNCS coordina su acción con otras autoridades nacionales. Este servicio puede solicitarse en el sitio web de CNCS, por correo electrónico o por teléfono.
Pero, las compañías que enfrentan un incidente de ciberseguridad y que cuentan con algún apoyo especialmente de las compañías de seguridad y seguros están más protegidas y pueden resolver sus problemas de ciberseguridad más fácilmente porque pueden contar con un equipo especializado que sabe qué hacer y para resolver los problemas de ciberseguridad.

Cada empresa que cuenta con servicios/soluciones relacionadas con esta área tiene sus propios métodos, herramientas, controles, análisis, pruebas y cada caso es un caso.

3.3.4. España

El mundo de la ciberseguridad es extremadamente dinámico. Siempre surgen nuevas amenazas y se descubren nuevas vulnerabilidades, incluso cuando hace poco tiempo no se consideraban como tales. Estos hechos han hecho que los sistemas de comunicación de red y TI evolucionen para enfrentar estas circunstancias alarmantes. Por esta razón, existe una creciente demanda de nuevos sistemas para detectar y gestionar incidentes de seguridad que podrían tener un impacto en las instalaciones industriales. Cada incidente de seguridad cibernética que se captura permite identificar las vulnerabilidades del sistema, así como el proceso de gestión para responder. Como consecuencia, la experiencia brindada por los equipos en los CERT es muy valiosa.

Uno de los primeros desafíos a superar será el inconveniente y el impacto que las medidas de seguridad pueden tener en las operaciones diarias. Esto es particularmente relevante cuando existe la necesidad de una respuesta de emergencia. Si, en este caso, hay un retraso causado por las medidas de seguridad aplicadas, el resultado podría ser catastrófico. Además, las técnicas de ciberataque evolucionan permanentemente. Este hecho requiere que los operadores de las instalaciones se actualicen técnicamente incluso si tales desafíos no están directamente relacionados con sus trabajos. Como consecuencia, se deben desarrollar nuevos procedimientos de respuesta automática para detectar y prevenir incidentes de ciberseguridad. Sin embargo, existe una dificultad adicional porque los sistemas operativos en tiempo real tienen una capacidad limitada para registrar y almacenar datos sobre la situación antes y después de una amenaza, lo que reduce la evidencia forense cuando hay un incidente. La gestión de cada incidente puede ser extremadamente útil para prevenir eventos futuros, responderlos en un tiempo más corto y gestionar de manera más eficiente sus efectos. Teniendo en cuenta todo esto, se deben establecer nuevas herramientas y procedimientos para obtener y utilizar este conocimiento, de tal forma que las empresas contribuyentes no se vean dañadas por tal hecho.

El papel y la experiencia de CERT en España tiene una clave para desarrollar este elemento debido al conocimiento y las capacidades ya adquiridas que se pueden aplicar a este nuevo entorno, y respaldar el desarrollo de herramientas para:

- Detectar el incidente;
- Evaluar su relevancia y tamaño;
- Informe sobre el incidente en sí;
- Habilitar la comunicación entre todas las entidades involucradas;
- Asistencia técnica en la recuperación de los sistemas implicados;
- Identificar la causa raíz del incidente;
- Evitar futuros incidentes similares;
- Desarrollar mejoras y una base de conocimiento sobre las lecciones aprendidas;
- Apoyar el estudio forense del incidente.

Estos servicios deben ser apoyados por otros que también sostendrán el resto de iniciativas tales como:

- Anunciar e informar sobre ataques en curso;
- Identificar, estudiar, clasificar y publicar nuevas vulnerabilidades;
- Recomendar nuevas acciones para mejorar la ciberseguridad general;
- Desarrollar y catalogar soluciones de ciberseguridad disponibles para el mercado general;
- Desarrollar tecnologías y capacidades forenses.

3.4. ¿Identifica los principales riesgos/dificultades que enfrentan las personas todos los días en su trabajo con respecto a la ciberseguridad?

3.4.1. Austria

La evaluación de las tendencias para 2018 reveló un espectro muy amplio de observaciones y evaluaciones. Después de la categorización y agrupación, las evaluaciones de tendencias citadas con mayor frecuencia se pueden resumir de la siguiente manera:

- La situación de peligro está en aumento y **los ataques son cada vez más complejos** y frecuentes y la principal motivación detrás de los ataques es la monetización;
- **La seguridad en la nube se está convirtiendo en un problema crítico** y se espera que las empresas dependan cada vez más de los proveedores de la nube;
- La **Ley de seguridad de redes y sistemas de información y la Ordenanza básica de protección de datos impondrán considerables demandas a las empresas**;
- La importancia de las **medidas organizativas (por ejemplo, la gestión de riesgos) aumentará en el futuro** en comparación con las medidas puramente técnicas;
- Se presupone que no se puede proteger completamente de los ataques y es importante reconocer los ataques rápidamente y reaccionar correctamente;
- La **dependencia de las empresas de productos de hardware y software** también representa una amenaza creciente.

3.4.2. República Checa

Las principales amenazas que las personas en el trabajo enfrentan con mayor frecuencia son:

- **Volúmenes crecientes de datos (Big Data) y la cuestión de la gobernanza y la seguridad de dicha cantidad de datos.** La protección y la seguridad de los datos son muy importantes para la República Checa, especialmente aquellos que son de interés público. En el sector público y privado, la cantidad de datos está creciendo y es necesario continuar almacenando más datos. Por lo tanto, comenzaron a usar nuevas formas de almacenamiento de datos, por ejemplo, almacenamiento en la nube. Sin embargo, un mayor uso de estos servicios en línea y en la nube a menudo conduce a una solución de seguridad no transparente cuya credibilidad puede ser cuestionable;
- **Diversidad de dispositivos móviles ("traiga su propio dispositivo").** Una amenaza interna significativa es una tendencia preocupante de la creciente aceptación del modelo "traiga su propio dispositivo". Con el objetivo "traiga su propio dispositivo", las empresas inicialmente infectan los dispositivos de los empleados personales que no implementaron medidas de seguridad estrictas y luego a través de ellos coloca el

troyano que infecta la red. Las políticas sobre el uso de hardware propiedad de los empleados deben examinarse a fondo y, cuando sea necesario, actualizarse y ampliarse;

- **Seguridad y privacidad de los servicios en la nube.** Los ataques a los servicios en la nube están ganando fuerza y se espera una gran violación de la seguridad en la nube en el futuro cercano. Hoy en día, las tres cuartas partes de las violaciones de seguridad duran días, semanas o incluso meses antes de ser descubiertas y, por lo tanto, aumentan en gran medida los daños del ataque;
- **Necesidad de rastrear el movimiento de datos dentro de la organización.** Las tecnologías de análisis de comportamiento permiten a las compañías e instituciones monitorear a los usuarios dentro de las compañías y a los usuarios finales. Esto puede advertirles sobre un comportamiento sospechoso que podría resutlar en robo de datos o ataques de software malicioso;
- **Ataques para destruir.** Algunos grupos *hacktivistas* ideológicamente perfilados sostuvieron que continuarán intentando atacar destructivamente contra los intereses de ciertas compañías o instituciones públicas;
- **Riesgos de seguridad asociados con la informatización de la administración pública (administración electrónica).** Por ejemplo, el proceso de adquisición electrónica conllevará nuevos riesgos que pueden amenazar la credibilidad del procedimiento de adquisición y los riesgos de seguridad asociados con el hecho de que las herramientas electrónicas para la adquisición están conectadas a la red pública.

La mejor manera de determinar la respuesta a incidentes apropiada en cualquier situación dada es comprender **qué tipos de ataques pueden usarse.** Se proporciona la lista de los diferentes vectores de ataque que enfrentan las personas en su trabajo con respecto a la ciberseguridad:

- **Dispositivos externos/extraíbles:** un ataque ejecutado desde medios extraíbles (por ejemplo, unidad flash, CD) o un dispositivo periférico;
- **Correo electrónico:** un ataque ejecutado a través de un mensaje de correo electrónico o archivo adjunto (por ejemplo, infección de malware);

- **Desgaste** Un ataque que emplea métodos de fuerza bruta para comprometer, degradar o destruir sistemas, redes o servicios;
- **Uso incorrecto:** cualquier incidente que resulte de la violación de las políticas de uso aceptable de una organización por parte de un usuario autorizado, excluyendo las categorías anteriores
- **Web:** un ataque ejecutado desde un sitio web o una aplicación basada en la web (por ejemplo, descarga automática);
- Pérdida o robo de equipos: la pérdida o robo de un dispositivo informático o medio utilizado por la organización, como un ordenador portátil o un teléfono inteligente.

3.4.3. Portugal

En Portugal, los principales riesgos y dificultades que los trabajadores pueden enfrentar en su vida profesional son los siguientes:

- **Ataques web que la principal motivación detrás está relacionada con la monetización y la difusión de información confidencial/privada;**
- **Suplantación de identidad;**
- **Correo no deseado;**
- **Infecciones de malware a través del correo electrónico;**
- **Ataques basados en la web;**
- **Seguridad y privacidad en la nube;**
- **Gestión de la privacidad de datos;**
- **Exposición a ataques informáticos, fallos del sistema y violación de datos;**
- **Perfil de riesgo global de las empresas** (algunos sectores de actividad están más expuestos que otros);
- La **falta de conocimiento para detectar información falsa** que puede conducir a, por ejemplo, infecciones y robo de datos;
- Un **ataque web** ejecutado desde alguna fuente no confiable;
- El **aumento en el uso de productos de hardware y software** también representa una amenaza creciente también.

3.4.4. España

Los principales riesgos dificultades que enfrentan los españoles hoy en día son:

- **Malware**;
- **Ataques basados en la web.** Dado que la mayoría de las operaciones comerciales se llevan a cabo en línea, los ataques basados en la web están en constante aumento. Los ciberdelincuentes se están volviendo más innovadores y utilizan técnicas sofisticadas para explotar vulnerabilidades sin parches en las aplicaciones web. El motivo detrás de estos ataques puede ser diferente: robar información confidencial de una empresa, mostrar anuncios de spam en el sitio web o descargar malware en el ordenador del usuario;
- **Los ataques a aplicaciones web** plantean una serie de problemas de seguridad derivados de la codificación inadecuada. Las debilidades o vulnerabilidades graves permiten a los delincuentes obtener acceso directo y público a las bases de datos para generar datos confidenciales. Muchas de estas bases de datos contienen información valiosa (por ejemplo, datos personales y detalles financieros), lo que las convierte en un blanco frecuente de ataques;
- **Violaciones de datos;**
- **Suplantación de identidad;**
- **Correo no deseado**;
- **Negación de servicio;**
- **Botnets**.

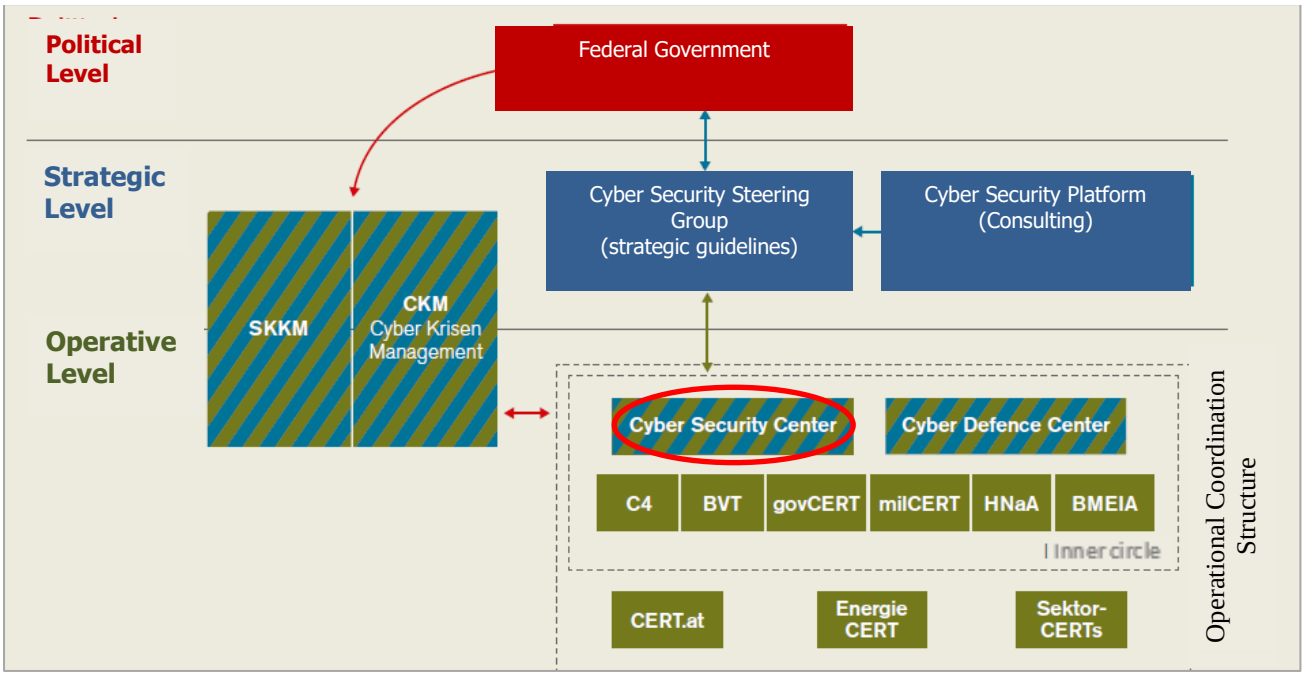
3.5. ¿Qué se está aplicando en su país para mejorar la seguridad de Internet de los ciudadanos en su trabajo?

3.5.1. Austria

Para proteger el ciberespacio y las personas en el espacio virtual, la Österreichischen Strategie für Cyber Sicherheit - Estrategia austriaca para la seguridad cibernética (ÖSCS) proporciona, entre otras cosas, la creación de una estructura de coordinación a nivel operativo. La estrategia INNEN.SICHER también cita la ciberseguridad como un desafío clave.

Como resultado, el proyecto INNEN.SICHER "Cyber Security. BVT" se lanzó en junio de 2014, cuyo elemento central es el establecimiento de un CSC en el Ministerio Federal del Interior. Este proyecto se completó con éxito en diciembre de 2017 con la transferencia del CSC a la operación regular. La importancia del proyecto se destaca, entre otras cosas, por el hecho de que la UE ha proporcionado una considerable financiación del Fondo de Seguridad Interior.

Figura 16 - Cibersefuridad en las compañías



Source: (Cyber Sicherheit Steuerungsgruppe, 2018)

Las tareas centrales del CSC se basan en cuatro pilares: la red y la autoridad de seguridad de la información; prevención y protección de infraestructuras críticas; coordinación y gestión de crisis cibernéticas; y, competencia técnica y personas de contacto.

Una tarea central esencial es la implementación del trabajo de prevención integral a través de:

- **Eventos de concienciación;**
- **Lecturas;**
- **Entrevistas de asesoramiento;**
- **Buena cooperación con la industria y las estructuras existentes** en el campo de la ciberseguridad en Austria.

El portal de seguridad de las TIC onlinesicherheit.gv.at es una iniciativa en cooperación con la economía austriaca y funciona como un portal central de Internet para temas relacionados con la seguridad en el mundo digital. Como medida de la estrategia nacional de seguridad de las TIC y la estrategia austriaca para la ciberseguridad, la iniciativa persigue el objetivo de promover y fortalecer de manera sostenible la cultura de las TIC y la ciberseguridad en Austria:

- **Sensibilizar y sensibilizar a los grupos destinatarios interesados** y proporcionarles recomendaciones de acción específicas para cada grupo destinatario;
- **Proporcionar una gama de información y servicios** en oferta está en constante expansión en el marco de reuniones editoriales periódicas con los 39 socios de cooperación (ministerios federales, gobiernos provinciales, autoridades, universidades de ciencias aplicadas, institutos de investigación, empresas, asociaciones y grupos de interés). Contiene las últimas noticias y advertencias, consejos e información adicional para principiantes y expertos;
- **Información a través de artículos de noticias, publicaciones y entradas de eventos.** En 2018, cada mes, se definió un tema central sobre las tendencias actuales, con un total de 34 artículos especializados publicados;
- **Actividades de formación (cursos);**
- **Medidas preventivas y trabajo de investigación intensivo;**
- **Aumento del trabajo preventivo y proyectos policiales como "CyberKids" y "Click & Check".**

3.5.2. República Checa

A medida que la digitalización continúa, cada empresa es naturalmente menos resistente a los riesgos de seguridad virtual. Los expertos en la República Checa definieron cinco reglas de ciberseguridad para las empresas:

- **Las empresas deberían crear un equipo de seguridad especial e incluirlo en medidas estratégicas;**

- **Involucrar a los empleados para que participen** en los resultados puede ser uno de los pasos más confiables que se pueden tomar;
- **Protección al cliente.** Debido a la interconexión de las oficinas del futuro, las empresas deberían ayudar a sus clientes a comprender cómo pueden protegerse no solo de los problemas legales. Las organizaciones deberían tratar activamente de comprender las implicaciones de la legislación nueva y próxima para que puedan asesorar a los clientes adecuadamente;
- **Las empresas deben trabajar con sus socios, proveedores y otros terceros** para compartir conocimientos, productos y servicios relacionados con la ciberseguridad;
- **Las empresas rara vez están dispuestas a compartir información o colaborar con otros**, pero la información que pueden dar sobre un ciberataque que sufren es muy importante para que múltiples partes interesadas sepan y piensen qué pueden hacer para evitar un ciberataque similar.

Hoy, una parte común de la gestión de la empresa es el Sistema de Gestión de Seguridad de la Información. Los elementos básicos utilizados en los sistemas internos de protección de redes comerciales son:

- **Protección antivirus a nivel de estación de trabajo**, por ejemplo, a nivel de puertas de enlace de Internet;
- **Protección antivirus para servidores de archivos y entornos de groupware;**
- **Protección antivirus para la comunicación de la puerta de enlace de Internet;**
- **Protección antispam por correo electrónico;**
- **Sistemas de detección y prevención de intrusiones.** Estas son herramientas de seguridad bastante sofisticadas que pueden detectar (IDS) un ataque continuo y tomar medidas para eliminarlo (IPS). La implementación de estos sistemas es más larga y exigente, lo que a menudo desalienta a los administradores a usarlos de manera consistente.

3.5.3. Portugal

Las buenas prácticas más comunes que las personas tienen en su trabajo son:

- **Participación en eventos** como C-DAYS que es un evento de referencia nacional que enfoca uno de los grandes temas relacionados con la seguridad de la información y el ciberespacio;
- Uso de **software antivirus en ordenadores;**
- Acceso a **la información a través de revistas, sitios web y medios generales;**
- **Sesiones de concienciación en múltiples temas** sobre ciberseguridad;sobre ciberseguridad;
- **Seminarios** relacionados también con la ciberseguridad que también promueven la promoción de proyectos, el debate y el intercambio de ideas;
- **Concienciación y participación en el programa de capacitación en ciberseguridad** a través de CNCS, que tiene como objetivo masificar la capacitación y la concientización;
- **Uso de equipos especiales de seguridad** presentes en la propia empresa (no tan frecuente) y a través de una empresa especializada en seguridad subcontratada;
- La **posibilidad de notificar y obtener ayuda** ante la eventual presencia de algún incidente;
- **Actividades de capacitación general** (cursos y talleres) que ocurren cada vez de una manera;
- **Entrenamiento interno por parte de algún miembro del equipo.**

3.5.4. España

Para mejorar la seguridad, se están implementando varias responsabilidades que se detallan a continuación:

- **La participación de las empresas en todas las iniciativas** de tal manera que puedan contribuir con su experiencia y conocimiento;
- **Desarrollo de programas de habilitación, herramientas, técnicas y documentos de referencia que puedan respaldar el desempeño de los profesionales de ciberseguridad.** Entre tales técnicas de referencia, se deben

desarrollar metodologías de implementación, políticas y procedimientos de seguridad cibernética, así como guías de mejores prácticas para cada sector industrial;

- **Organización de iniciativas de capacitación, manuales gratuitos y talleres** que tengan en cuenta las diferentes necesidades de todos los roles relacionados, debe hacerse especial hincapié en los profesionales de TI que desean involucrarse en la protección de las plantas de automatización y los sistemas de control. Deben considerarse las necesidades de capacitación de los profesionales e ingenieros de control que desean diseñar de manera segura las nuevas infraestructuras de control y automatización;
- **Publicar informes de análisis en profundidad a nivel ejecutivo sobre los beneficios de seguridad cibernética;**
- **Supervisión y monitoreo constante de los hitos y avances que pueden tener un efecto en la ciberseguridad industrial** para asegurar la efectividad de las acciones ejecutadas.

En este sentido, podemos destacar la trayectoria del Grupo Telefónica, que a principios de siglo comenzó a formar la línea de Ciberseguridad y ahora cuenta con 16 CSIRT repartidos por todo el mundo. Además, la empresa filial experta en ingeniería "Next" que pertenece al grupo BBVA impulsará la transformación tecnológica del banco BBVA. Para ello cuenta con expertos avanzados en análisis de masas y macrodatos, IA, blockchain y ciberseguridad. En lo que respecta a la ciberseguridad, cuentan con un equipo solvente que ofrecerá servicios de seguridad profesionales avanzados que incluyen soluciones de infraestructura y aplicaciones, desarrollo de software seguro y soluciones de ciberseguridad tanto para el Grupo BBVA como para las empresas líderes.

4. Seguridad en Internet e Industria 4.0: en la vida privada

4.1. ¿Qué accidentes relacionados con la seguridad en Internet se resolvieron en su país en los últimos años en la vida privada de los ciudadanos?

4.1.1. Austria

No hubía información sobre este tema para Austria.

4.1.2. Czech Republic

Los ataques más comunes en la vida privada de los ciudadanos son:

- **Virus:** el virus más común se puede propagar a través de archivos adjuntos de correo electrónico y mensajes de texto, descargas de archivos de Internet y enlaces de estafa de redes sociales;
- **Gusano:** los gusanos de correo electrónico generalmente se propagan creando y enviando mensajes salientes a todas las direcciones en la lista de contactos de un usuario;
- **Estafa:** algunas de las estafas más comunes son: phishing; estafa de donación (una persona que dice tener ellos o tener un hijo o alguien que conoce con una enfermedad y necesita asistencia financiera); bagre (una persona que crea un perfil falso en línea con la intención de engañar a alguien); y, correo en cadena que generalmente es inofensivo y se propaga a través del correo electrónico y le dice a la gente que reenvíe el correo electrónico;
- **Spam:** la mayoría de los mensajes de spam son comerciales. Ya sea comercial o no, muchos no solo son molestos sino también peligrosos porque pueden contener enlaces que conducen a sitios web de phishing o sitios que alojan malware o incluyen malware como archivos adjuntos;
- **Suplantación de identidad.**

4.1.3. Portugal

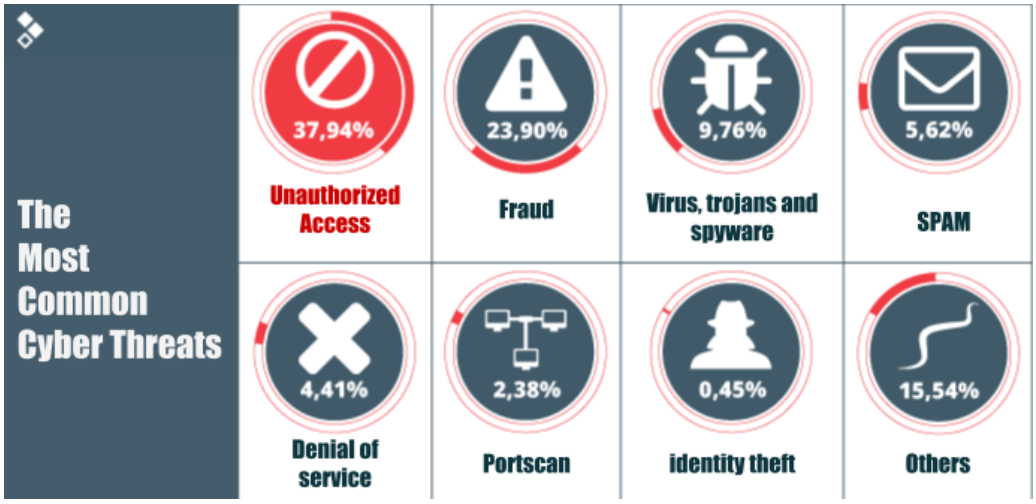
Los incidentes más comunes que enfrentan las personas en su vida privada son:

- **Virus**;
- **Suplantación de identidad.**
- **Correo no deseado;**
- **Acceso no autorizado;**
- **Identidad hábil, especialmente en las redes sociales.**

4.1.4. España

Los ciberataques más comunes, como podemos ver en la siguiente figura, son: acceso no autorizado y fraude.

Figura 17 - Incidentes más comunes



Fuente: (INCIBE, n.d.).

4.2. ¿Existen en su país equipos para monitorear la seguridad en Internet y la ciberseguridad con respecto a los ciudadanos en su vida privada?

4.2.1. Austria

En Austria, el equipo responsable de supervisar la seguridad en Internet y la ciberseguridad para los ciudadanos es el Centro de Competencia en Delitos Cibernéticos (C4). El Cyber Crime Competence Center (C4) es el centro nacional e internacional de coordinación y presentación de informes para combatir el delito cibernético. El Centro está formado por expertos técnicos y profesionales altamente especializados de los campos de investigación, medicina forense y tecnología. El Cyber Crime Competence Center C4 se estableció en 2011 para combatir el delito informático como una unidad separada dentro del Departamento de Investigación Criminal de la Oficina Federal de Policía Criminal. Cyber Crime Competence Center C4 se divide en cuatro unidades: "Tareas centrales"; "Salvaguardar la evidencia de TI"; "Investigaciones"; "Desarrollo e innovación"; y, la oficina de informes.

Figura 18 - Logo cyber crime center

Fuente: (Bundeskriminalamt[1], 2019)

La Oficina de Informe de Delitos Cibernéticos del (C4) es, por un lado, el punto de contacto para la población. Esto permite identificar nuevos fenómenos en una etapa temprana. Por otro lado, también es la interfaz con el CSC y un punto de contacto internacional en materia de delitos cibernéticos. Otra tarea importante es actuar como punto de contacto para todos los servicios policiales en relación con el delito cibernético (Cyber Sicherheit Steuerungsgruppe, 2018).

4.2.2. República Checa

La asociación NarodniCentrumBezpecnejsiholInternetu (NCBI) es miembro de la red paneuropea de centros nacionales de sensibilización más seguros INSAFE. En colaboración con sus socios, NCBI organiza conferencias, seminarios, lecturas y sesiones de capacitación relacionadas con el uso más seguro de Internet y la prevención del delito en Internet en la República Checa.

Figura 19 - Logo NCBI

Fuente: (S@ferinternet.cz, n.d.)

El Centro para la prevención de la comunicación virtual arriesgada es un instituto que se ocupa de las formas arriesgadas de comunicación en línea de niños y adultos. Se centra en el acoso cibernético, el acecho, los engaños y el correo no deseado; sexting; ingeniería social en la comunidad en línea; el riesgo de compartir datos personales en redes sociales; y, otros fenómenos de comunicación peligrosos.

4.2.3. Portugal

En Portugal hay algunas instituciones que pueden ayudar a la sociedad portuguesa a prevenir incidentes de ciberseguridad. Las instituciones pueden verse de la siguiente manera:

En Portugal, hay dos entidades que promueven la seguridad web y la protección de datos personales:

- **CNPD:** el primero y el más conocido es CNPD, que es una entidad administrativa independiente con poderes de autoridad que trabaja con la Asamblea de la República. La CNPD coopera con las autoridades supervisoras de protección de datos de otros estados, es decir, en la defensa y el ejercicio de los derechos de las personas que viven en el extranjero. Además, el CNPD es el organismo facultado para supervisar y controlar el cumplimiento de las leyes y reglamentos dentro del área de protección de

datos personales con estricto respeto por los derechos humanos y la libertad. CNSC quiere garantizar la libertad, la seguridad y un ciberespacio de justicia para todos. A corto plazo, este consorcio ofrece algunas respuestas para prevenir eventos adversos. A medio/largo plazo, el objetivo es desarrollar buenas prácticas en materia de ciberseguridad.

Figura 20 - Logo CNPD

Fuente: (CNPD, n.d.)

- **Asociación "Associação dos Profissionais de Proteção e de Segurança de Dados":** es una asociación profesional que representa a individuos y organizaciones que se ocupan de la protección y la seguridad de los datos, la privacidad y la regulación de la comunicación electrónica o que ocupan el cargo de oficiales de protección de datos en organizaciones que operan en territorio portugués

4.1.4. España

INCIBE-CERT es uno de los equipos de respuesta a incidentes de referencia que mejora la eficiencia en la lucha contra los delitos que involucran redes y sistemas de información, reduciendo sus efectos en la seguridad pública. La misión de INCIBE es fortalecer la ciberseguridad, la confianza y la protección de la privacidad con respecto a los servicios ofrecidos dentro de la sociedad de la información, proporcionando valor al público, las empresas, el gobierno español, la red académica y de investigación española, el sector de tecnología de la información y los sectores estratégicos en general.

INCIBE es el centro de referencia de respuesta a incidentes de seguridad para ciudadanos y entidades de derecho privado en España, operado por el Instituto Nacional de Ciberseguridad

de España, dependiente del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el avance digital. Como centro de excelencia, INCIBE es un servicio ofrecido por el gobierno español para trabajar hacia el desarrollo de la ciberseguridad como instrumento para la transformación social y para desarrollar nuevos campos de innovación. Con este fin, con sus actividades centradas en la investigación, la prestación de servicios y la cooperación con los actores relevantes, INCIBE lidera una serie de iniciativas dirigidas a la ciberseguridad a nivel nacional e internacional.

Figura 21 - Logo incibe

Fuente: (Incibe.es, n.d.)

4.3. ¿Qué hacen los ciudadanos en su país cuando enfrentan un incidente de seguridad cibernética?

4.3.1. Austria

En Austria hay varias líneas directas específicas para cada tema a las que puede recurrir si se ha convertido en una víctima de delitos relacionados con TI. Dependiendo del tipo de incidente de ciberseguridad, las personas pueden confiar en diferentes autoridades. También hay algunas instituciones que brindan información importante (por ejemplo, consejos) para evitar incidentes de ciberseguridad.

- **The Watchlist Internet:** esta institución enumera en su sitio web numerosos artículos sobre varios intentos de fraude, como tiendas falsas, phishing, facturas falsas y trampas de suscripción. Esta es también una lista de tiendas en línea fraudulentas, que siempre se mantiene actualizada. Esta es la institución con la que las personas de Austria pueden ponerse en contacto si tienen un incidente de estafa y fraude;

- **Defensor del Pueblo de Internet:** esta oficina de informes ofrece ayuda con la resolución de disputas, así como asesoramiento gratuito en línea sobre todos los aspectos de las compras en Internet. El Defensor del Pueblo de Internet es un organismo de conciliación aprobado por el estado para disputas que surgen de contratos en línea bajo la Ley Alternativa de Resolución de Disputas. También ofrece arbitraje gratuito y asesoramiento sobre otros temas relacionados con Internet (derechos de autor, ley de protección de datos, derecho a la propia imagen, derechos personales, etc.) (Bundesministerium für Digitalisierung und Wirtschaftsstandort1, 2019);
- **Trabajo de la policía criminal:** se ha creado una oficina especial de denuncia para proporcionar información a los ciudadanos si tienen que luchar contra una situación de delito cibernético. Además, si una persona tiene sospechas o indicaciones concretas de cibercrimen, puede comunicarse con la oficina de informes pertinente del Ministerio Federal del Interior (Bundesministerium für Digitalisierung und Wirtschaftsstandort1, 2019).
- **Saferinternet.at:** Saferinternet.at es el punto de información y coordinación austriaco en la red de Internet más segura de la UE. Apoya a los usuarios de Internet con consejos y asistencia en el uso competente y seguro de Internet, teléfonos móviles y juegos de ordenador. La iniciativa está dirigida específicamente a niños, jóvenes, padres y maestros (Bundesministerium für Digitalisierung und Wirtschaftsstandort1 2019);
- **Línea directa de seguridad cibernética:** en caso de emergencia (por ejemplo, un ataque cibernético o el cifrado de sus datos por un troyano), la línea directa de seguridad cibernética en el 0800 888 133 puede proporcionar asistencia gratuita durante todo el día;
- **Comisión de seguridad de la información:** en la Cancillería Federal actúa como un punto de contacto reconocido a nivel nacional e internacional por la Autoridad de Seguridad Nacional para todas las preguntas en el campo de la seguridad de la información y las áreas relevantes, tales como seguridad del personal, seguridad física, seguridad de documentos o gestión de registros y seguridad de la información, así

como un organismo nacional de acreditación para instituciones nacionales en relación con el procesamiento de información clasificada (Bundesministerium für Digitalisierung und Wirtschaftsstandort2, 2019).

4.3.2. República Checa

La ciberseguridad es un fenómeno global que representa un desafío para todas las personas. Aunque la ciberseguridad es uno de los desafíos más importantes que enfrentan los gobiernos en la actualidad, la visibilidad y la conciencia pública siguen siendo limitadas. Casi todos han oído hablar de la ciberseguridad, sin embargo, la urgencia y el comportamiento de las personas no reflejan un alto nivel de conciencia. Algunas medidas principales que sigue el público:

- **Tener un sistema operativo legal y actualizado regularmente;**
- **Use software antivirus y firewall;**
- **Actualice su navegador web regularmente;**
- **Utilizar las extensiones de seguridad del sistema de nombres de dominio** que proporcionan autenticación de origen de datos;
- **Utilizar una contraseña segura.**

4.3.3. Portugal

Si hay una situación en la que las personas enfrentan un incidente de seguridad cibernética, pueden contactar a algunas instituciones. Estas instituciones se mencionan a continuación:

- **Asociación "APDPO Portugal - Associação dos Profissionais de Proteção e de Segurança de Dados":** es una asociación profesional que representa a individuos y organizaciones que se ocupan de la protección y la seguridad de los datos, la privacidad y la regulación de la comunicación electrónica o que ocupan el cargo de oficiales de protección de datos en organizaciones que operan en territorio portugués;
- **Línea telefónica de contacto "internet segura":** la asociación Associação Portuguesa de Apoio à Vítima es responsable de la gestión y puesta en funcionamiento de esta línea. El objetivo principal de esta línea telefónica y en línea es ayudar y responder a las dudas y problemas relacionados con la seguridad en línea, el acoso

cibernético, la intimidación y la exposición indigna para jóvenes, adultos, maestros y niños. El soporte completo es confidencial y anónimo;

- **Contactar con la línea telefónica "Linha aberta":** esta línea telefónica se centra en el contenido ilegal (pornografía infantil, violencia y racismo) y el enjuiciamiento penal de quienes publican este tipo de contenido;
- **Contactar con los oficiales de policía**, si es necesario.

Sin embargo, es importante decir que las personas tienen acceso libre a algunas iniciativas (por ejemplo, medidas, talleres, cursos, tutoriales ...) para prevenir incidentes de ciberseguridad.

4.3.4. España

La detección temprana de incidentes es la piedra angular para apoyar acciones y procedimientos para detener su expansión y efectos y facilitar la recuperación. Para detectar estas acciones dañinas de manera sistemática, será necesario desarrollar e implementar agentes de detección, así como herramientas centralizadas de gestión de eventos. Un incidente, una vez que se detecta, debe identificarse y valorarse dentro de su tipo e impacto. Debe desencadenar un procedimiento de respuesta automatizada; para conocer el personal o las instalaciones potencialmente dañadas sobre la naturaleza del incidente y las características principales. También debe ofrecer información detallada para tomar las decisiones apropiadas para su gestión y desplegar las siguientes medidas de detención apropiadas:

1. Replantear parámetros de seguridad;
2. Asegurar los datos confidenciales;
3. Prevenir ataques, de forma integrada mediante la implementación de medidas cibernéticas;
4. Incorpora funcionalidades clave para interactuar con estos dispositivos sin riesgo. Estas funcionalidades asegurarán accesibilidad, integridad, confidencialidad y control de acceso;
5. Clasificar posibles riesgos y amenazas;

6. Incluye software altamente confiable.

4.4. ¿Identifica los principales riesgos/dificultades que enfrentan las personas todos los días en su vida privada con respecto a la ciberseguridad?

4.4.1. Austria

Los principales riesgos/dificultades que enfrentan las personas todos los días en su vida privada son:

- **Suplantación de identidad** a través del robo de datos;
- **Ransomware (blackmailstrojan, cryptotrojan):** prácticamente toma al ordenador infectado como rehén y encripta datos individuales y carpetas;
- **Troyanos:** pasan desapercibidos en el ordenador y trabajan en segundo plano para enviar correos no deseados o ataques DDoS contra ciertos sitios web o empresas;
- **Virus y gusanos:** lo que un virus o gusano finalmente hace con su propio ordenador no puede predecirse ni limitarse. Al principio, a menudo había virus de broma que se desvanecían en los mensajes o apagaban el PC. Sin embargo, dicho delincuente puede simplemente eliminar o cifrar todos los datos;
- **Acoso en línea**, acoso cibernético;
- **Estafadores en compras en línea** (tiendas falsas, falsificación de marcas);
- **Trampas de suscripción, términos y condiciones ocultos;**
- **Fraude publicitario clasificado:** empresas inexistentes que envían mensajes falsos y luego pagan dinero sin recibir los productos;
- **Configuraciones de privacidad y protección de datos;**
- **Farsa/carta en cadena.**

4.4.2. República Checa

Las tendencias del delito cibernético se obtuvieron de los informes anuales publicados entre 2011 y 2016, que se publican anualmente por el Departamento de Política de Seguridad del Ministerio del Interior. Cada informe sobre la situación en el campo de la seguridad interna y

el orden público en la República Checa (hasta 2016) describe, entre otros, el delito de información y la ciberseguridad del año anterior. Para el período 2010 a 2015, con la excepción de 2010, todos los informes contienen datos cuantificados sobre delitos de información.

Las manifestaciones más comunes de este delito idéntico son:

- **Violaciones de derechos de autor;**
- **Difusión de propaganda extremista y terrorista;**
- **Difusión de pornografía prohibida;**
- **Conducta fraudulenta;**
- **Amenazas;**
- **Chantaje;**
- **Alarmismo;**
- **Calumnia;**
- **Ataques a sistemas de información y datos;**
- **Acecho;**
- **Extorsión y estafa;**
- **Manipulación no autorizada de datos;**
- **Estafa** (casos de fraude en la tecnología de la información y especialmente en Internet).

El número total de incidentes cibernéticos está creciendo desde 2011 (consulte la tabla anterior). En 2015, el número de incidentes cibernéticos fue de 5023 casos.

Figura 22 - Número de incidentes cibernéticos (características de series de tiempo)

year	number of incidents	absolute growth	relative growth	growth coefficient
2011	1502	-	-	-
2012	2195	693	0.461385	1.461385
2013	3108	913	0.415945	1.415945
2014	4348	1240	0.39897	1.39897
2015	5023	675	0.155244	1.155244

Fuente: Sociálno-Ekonomická revue (2017)

4.4.3. Portugal

Hoy en día, los principales riesgos que enfrentan las personas todos los días en su vida privada con respecto a la ciberseguridad son:

- **Virus y gusanos informáticos;**
- **Infecciones de malware a través del correo electrónico;**
- **Software malicioso**;
- **Suplantación de identidad;**
- **Troyano**;
- **Gusano**;
- **Virus**;
- **Correo no deseado**;
- **Enlaces fraudulentos**;
- Personas que **facilitan información personal en línea**, como EL Documnto Nacional de Identidad, detalles de pago, tarjeta de crédito/débito o número de cuenta bancaria;
- La **utilización abusiva de información personal;**
- **El acceso de los niños a contenido digital inapropiado;**
- La **falta de limitación a las cookies** debido a la falta de conocimiento.

4.4.4. España

La falta de conocimiento sobre el entorno de información digital constituye una vulnerabilidad de la opinión pública española. Aquí hay una lista de algunos de los problemas clave que las personas tienen que enfrentar todos los días:

- **Secuestro de datos.** Los métodos de infección con *ransomware* son:
  - **Escritorio remoto:** nueva forma de infectar ordenadores con *ransomware*. Permite el acceso remoto al sistema, que se infectará más adelante;
  - **Dispositivos móviles:** el volumen de *ransomware* móvil se multiplicó por tres durante el último año;
  - **Correo electrónico:** es el medio más popular para distribuir *ransomware* porque no existe un método apropiado para garantizar la protección;
  - **Explotaciones**: se utilizan para infectar sistemas. Un ejemplo de esto se vio en bases de datos mal protegidas, como los ataques Mongo DB;

  - **Televisores:** se observaron casos de *ransomware* relacionados con la infección de televisores convencionales, como resultado de la nueva sofisticación de estos ataques;
  - **Medjack:** secuestro de dispositivos médicos, resultado de la integración de las tecnologías tradicionales de TIC y salud.
- **Ataques distribuidos de denegación de servicio (DDoS).** Los tipos de ataques más frecuentes son:
  - **Dispositivos IOT:** la cantidad de dispositivos IOT vulnerables ha contribuido al aumento en el tamaño de los ataques DDoS;
  - **DDoS como servicio:** en desarrollo, debido a la reducción en el costo de las herramientas necesarias para llevarlas a cabo;
  - **Extorsión:** acciones de extorsión bajo amenaza de ataques DDoS o interrupción de servicios en línea.
- **Hacktivismo.** Estos ataques pueden ser aún más dañinos que las amenazas tradicionales porque los *hacktivistas* a menudo intentan hacer una declaración, por lo que sus esfuerzos suelen ser muy perjudiciales para la reputación de una organización;
- **Botnets.** La piratería en dichos sistemas se volverá más común en los próximos años con *ransomware* y *hacktivismo* que se consideran áreas problemáticas clave. También existe una importante amenaza a la privacidad, ya que los dispositivos inteligentes suelen contener una cantidad considerable de información confidencial a la que los ciberdelincuentes pueden acceder;
- **Manipular o engañar a personas** clave para que divulguen datos importantes o información financiera, como a través de técnicas de *phishing*;
- **Amenazas internas (acceso a información confidencial).** Existe una posibilidad significativa de que surjan problemas de ciberseguridad internamente. La mayoría de las amenazas externas son fáciles de reconocer e identificar. De estos, más de dos tercios eran personas con intenciones maliciosas, mientras que los incidentes restantes se debieron a "actores involuntarios". Este último se refiere a personas inocentes que accidentalmente permitieron a los atacantes acceder a la información, o que no siguieron las medidas de seguridad;

- **Malware móvil;**
- **Anuncios y comentarios falsos.** Los consumidores son frecuentemente bombardeados con anuncios en línea y la proliferación de anuncios falsos y ataques de *phishing* han erosionado la confianza en las garantías de marketing basadas en la red;
- **Servicios y computación basados en la nube;**
- **Flujo de información entre varios dispositivos.** La mayoría de los empleados de hoy traerán sus propios dispositivos al trabajo, por ejemplo, teléfonos inteligentes, tabletas y ordenadores portátiles. Pero si estos dispositivos se duplican como dispositivos personales y de trabajo, esto podría comprometer la información o los datos confidenciales de su empresa;
- **Gestión de credenciales de empleados.** Garantizar que solo los empleados y contratistas adecuados tengan acceso a información comercial confidencial o compartimentada puede ser la diferencia entre un entorno de seguridad sólido y ser víctimas de amenazas cibernéticas internas.

4.5. ¿Qué se está aplicando en su país para mejorar la seguridad de los ciudadanos en Internet en su vida privada?

4.5.1. Austria

En Austria existen algunas iniciativas para mejorar la seguridad en Internet de los ciudadanos en su vida privada. Algunos de ellos se pueden ver a continuación:

- **Folletos con consejos básicos** de seguridad para el uso correcto de Internet y ordenadores para la seguridad personal de TI. Estos consejos tratan los siguientes temas: protección del PC; correos electrónicos y chat; software; redes de intercambio de archivos; las compras en línea; pago; banca en línea en la web; información privada, fotos y contraseñas; ofertas como mercancía o agentes financieros; y aplicaciones y trampas de suscripción. Estos folletos son elaborados por la Oficina Federal de Policía Criminal de Austria;
- **Noticias.**

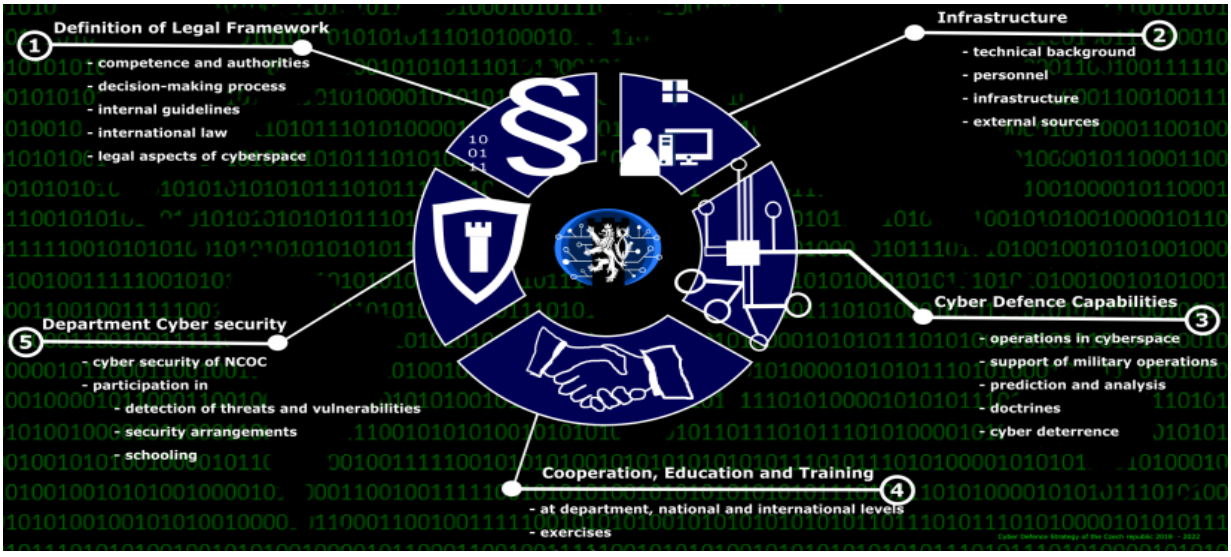
4.5.2. República Checa

Para mejorar la seguridad, se implementa la Estrategia de Seguridad Cibernética de la República Checa. La estrategia de seguridad cibernética para la República Checa abarca los años 2015 a 2020.

La Estrategia Nacional de Seguridad Cibernética de la República Checa es un documento que declara los valores centrales, intereses, actitudes, ambiciones y herramientas de la RC para salvaguardar la seguridad y formula los principios sobre los cuales se fundó la política de seguridad de la RC. En esta estrategia se definen los intereses vitales, estratégicos y otros intereses importantes de RC, el entorno de seguridad, así como también se describe el sistema de seguridad. La estrategia de seguridad es el documento básico de la política de seguridad de la RC. En el texto se destaca a nivel general también la ciberseguridad. Esta estrategia luego construye subestrategias y conceptos.

Los principios básicos de la estrategia de ciberseguridad: vincular y fortalecer la cooperación de todos los sectores de la sociedad; responsabilidad individual; cooperación departamental; cooperación internacional; adecuación de las medidas adoptadas; utilizar tecnología de información confiable; y, sensibilizar hacia la ciberseguridad.

Figura 23 - Estrategia de defensa cibernética de la República Checa (2018-2022)



Fuente: National Cyber Operations Center (n.d.)

También hay otras buenas iniciativas a mencionar como:

- **Proyecto de Internet más seguro:** el objetivo es crear conciencia sobre la seguridad de Internet, luchar contra el contenido ilegal, no deseado y dañino y crear conciencia entre los usuarios finales, los padres y los maestros. La lucha contra el contenido ilegal se centra en nuevos tipos de comunicación como las redes sociales. Los principales grupos objetivo del proyecto incluyen niños y jóvenes, padres, educadores, especialistas, etc. Más información en este sitio web: https://www.saferinternet.cz;
- **Proyecto E-Bezpečí:** el objetivo es crear conciencia sobre la prevención, la educación, la investigación, la intervención y el comportamiento arriesgado de Internet y los fenómenos relacionados. El proyecto también se centra en el uso positivo de TI en la educación y en la vida cotidiana en la República Checa. Más información en este sitio web: https://www.e-bezpeci.cz/.

4.5.3. Portugal

En Portugal existen algunas iniciativas para mejorar la seguridad en Internet de los ciudadanos en su vida privada. Algunos de estos ejemplos incluyen:

- **El consorcio "CNCS"** organiza múltiples iniciativas: consejos; recomendaciones; folletos sesiones de sensibilización; seminarios relacionados con la ciberseguridad y la promoción de proyectos; programa de sensibilización y formación relacionada con la ciberseguridad; evento nacional sobre área de seguridad digital que ocurre una vez al año; curso general de ciberseguridad y muchos más;
- **Dos líneas telefónicas** que ayudan a las personas si tienen dudas y problemas relacionados con la seguridad en línea, la ciberseguridad, el acoso y la exposición indigna para jóvenes, adultos, maestros y niños;
- **Sitio web en línea "SegurançaNet - Navegar em segurança"** que es similar a una base de datos (con presentaciones, audio, pdf y videos) orientada a niños, escuelas, jóvenes, padres y maestros. Con la iniciativa "Líderes digitais 2018-2019" que tiene como objetivo motivar a los estudiantes para la promoción de diferentes asignaturas que permitan una utilización más responsable de la tecnología y el entorno digital;

- **Sello de seguridad digital (etiqueta eSafety)** que otorga una certificación y apoya a las escuelas y tiene como objetivo promover un entorno seguro relacionado con la tecnología digital como una experiencia de enseñanza y aprendizaje;
- **Sitio web "Ensina RTP":** este es un sitio web en línea que tiene información (videos y noticias breves) para múltiples temas, como la seguridad de Internet;
- **Proyecto "Net Segura e Viva":** este proyecto tiene como objetivo ofrecer un repositorio muy útil (con información organizada en Preguntas frecuentes) con consejos de todas las áreas relacionadas con la ciberseguridad. Además de ser una plataforma en línea, Google y Deco Protest llevaron a cabo múltiples conferencias "NETtalks" sobre ciberseguridad en varias ciudades de Portugal. Esta iniciativa nacional también invita a todos los jóvenes a producir algunos videos que muestren la importancia de participar en las redes sociales con seguridad y respeto a la privacidad. Los videos producidos por los estudiantes deben promover la utilización segura de Internet de una manera creativa, especialmente en las redes sociales. Los mejores videos se hicieron públicos en el sitio web en línea;
- **Proyecto "Internet Segura":** con respecto al "Día Europeo de Internet Seguro" que ocurre todos los años, generalmente en febrero, dos compañías (Microsoft y Guarda Nacional Republicana) organizan un evento relacionado con este tema con muchas actividades en todo el país durante una semana;
- **Centro "Centro de Segurança Google":** desde 2018 Google dio acceso al "Centro de Segurança Google" para proteger a sus usuarios de amenazas como spam, software malicioso o virus. Este centro brinda información útil para ayudar a los portugueses a tener un mejor control, seguridad y privacidad sobre la navegación en línea y con esta iniciativa Google tiene como objetivo brindar información sobre muchos temas, especialmente para las familias;
- **APDPO Portugal - "Associação dos Profissionais de Proteção e de Segurança de Dados":** es una asociación profesional que representa a individuos y organizaciones que se ocupan de la protección y la seguridad de los datos, la privacidad y la regulación de la comunicación electrónica o que ocupan el cargo de oficiales de protección de datos en organizaciones que operan en territorio portugués;

- **Proyecto "Miúdos seguros na NET":** este fue un proyecto que ayudó a familias, escuelas y comunidades a promover la seguridad en línea para niños y jóvenes. Los principales recursos disponibles son artículos (entre 2003 y 2008) y un blog.

Además de estas iniciativas, algunas empresas promueven la divulgación de información relacionada con la seguridad de Internet en sus propios sitios web o blogs. En Portugal, también hay varios libros relacionados con la seguridad en Internet.
Sin embargo, aunque hay algunas actividades relacionadas con la seguridad en Internet, el gobierno portugués no tiene un papel activo cuando se trata de promover actividades de difusión. Si alguien con un problema relacionado con la protección de datos o la seguridad en Internet tiene que buscar una solución en línea, debe ponerse en contacto con un abogado o una persona que tenga más conocimiento relacionado con estos temas.

4.5.4. España

Para mejorar la seguridad, se están implementando varias responsabilidades que se detallan a continuación:

- **Proyecto Safer Internet Center Spain (SIC-SPAIN):** este proyecto continúa y amplía el servicio proporcionado por Internet Segura for Kids (IS4K). Promueve el uso seguro y responsable de Internet y las nuevas tecnologías entre niños y adolescentes. En línea con la estrategia europea BIK (Better Internet for Kids), forma parte de la red paneuropea INSAFE de centros de seguridad en Internet. En función de su interoperabilidad con la plataforma de servicios básicos, la financiación, en virtud de esta convocatoria, permitirá a los diversos SIC europeos mantener y expandir plataformas nacionales en toda la UE a través de los siguientes servicios:
- **Conciencia:** Un centro para crear conciencia entre los niños, padres, maestros y otros profesionales que trabajan con niños sobre los riesgos que pueden enfrentar a través de actividades en línea sobre la protección de menores. Se desarrollarán herramientas y servicios específicos de sensibilización en cooperación con terceros.

- **Línea de ayuda:** Servicios de ayuda en línea que brindan apoyo a jóvenes, padres, educadores y otros profesionales en el campo, en asuntos relacionados con la protección de menores en Internet.
- **Línea directa:** Servicio integral de denuncia ciudadana destinado a recibir y gestionar incidentes relacionados con imágenes y videos ilegales de abuso sexual infantil en línea.

Mejora de la coordinación entre los participantes del consorcio, así como con otros agentes presentes y activos en esta área para crear una plataforma público-privada en la que diferentes entidades se coordinen para desplegar acciones de sensibilización sobre el uso de Internet en menores con un impacto expandido en el nivel nacional.

5. Conclusiones

La Industria 4.0 está impulsada por tecnologías disruptivas y los impactos de esta nueva reindustrialización de muchas maneras, principalmente al proporcionar efectividad operativa y desafiar los modelos comerciales establecidos. Aunque son numerosos los beneficios en las áreas conectadas a la Industria 4.0, la cuarta revolución industrial trae consigo un nuevo riesgo operativo para los fabricantes inteligentes y conectados y las redes de suministro digital.

La naturaleza interconectada de la Industria 4.0 junto con la transformación de digitalización significa que los ataques cibernéticos pueden tener efectos mucho más extensos que nunca. Esto significa que es imperativo que las organizaciones comprendan completamente las implicaciones de estos riesgos de ciberseguridad antes de adoptar sus estrategias de ciberseguridad para ser más seguras, vigilantes y resistentes, así como integrarse completamente en las organizaciones.

Las organizaciones deben enfocarse y comprometerse con un marco que: brinde un enfoque integrado a la seguridad cibernética, desarrolle capacidades para la detección de amenazas para responder de manera adecuada y proactiva, el desarrollo de capacidades en recursos humanos para la Industria 4.0 debe involucrar una estrategia múltiple en los departamentos. Para lograr los beneficios reales de la cuarta revolución industrial, el gobierno y también las personas deberán tomar medidas para adaptarse a los riesgos en evolución.

Por lo tanto, los gobiernos nacionales y las instituciones públicas deberían desarrollar programas para mejorar las capacidades de la fuerza laboral y garantizar que el contenido de estos programas se modifique adecuadamente para incluir todas las materias básicas en el futuro. Además, las políticas públicas deberían dar incentivos adecuados a las empresas para invertir en esta área.

Cuando se trata de personas, también existe una gran necesidad de actualizar las medidas de seguridad interna para todos. Por lo tanto, la facilitación de la educación, la formación y el desarrollo de habilidades es igualmente fundamental. Además, ser resistente y tener una postura cuidadosa también conlleva la necesidad de que las personas estén más informadas porque un mundo seguro es una responsabilidad compartida por todos.

A continuación, tenemos una lista de las principales barreras/dificultades que enfrentan las empresas y los ciudadanos y algunas recomendaciones para mejorar la ciberseguridad.

5.1. Análisis comparativo entre todos los países.

La Industria 4.0 está promoviendo varios cambios en todo el mundo en las empresas, así como en la sociedad en general, y con esta nueva revolución industrial, la existencia de ataques aumentó sustancialmente. Como consecuencia, todos los países enfrentan todos los días algunos desafíos y ataques cibernéticos que se vuelven más complejos y surgen con mayor frecuencia.

Desde los últimos años, todos los países están involucrados en la organización de múltiples iniciativas que apuntan a mejorar la respuesta a los principales desafíos de esta nueva revolución industrial y la ciberseguridad. Las iniciativas más comunes relacionadas con este tema que están presentes en cada país son: planes estratégicos de país; posible acceso a algún apoyo financiero; acceso a la información a través de algunas plataformas; la existencia de una autoridad pública que ayuda con la protección de datos y la ciberseguridad en cada país (como los CERT); proyectos de ciberseguridad (públicos y privados); y, la existencia de información nacional (por ejemplo, directrices, orientaciones, ...). A pesar de todas las iniciativas que existen, todos los países aún enfrentan numerosos desafíos y necesitan invertir más y hacer adaptaciones continuas día a día.

Además, algunos de los desafíos más comunes que enfrentan los países analizados son: la falta de competencias y la recalificación de los recursos humanos; falta de habilidades para detectar y lidiar con fallos de seguridad; falta de apoyo a través de las autoridades/organizaciones públicas; cooperación entre todos los organismos pertinentes a nivel nacional; La existencia de una base jurídica obsoleta.

Las amenazas cibernéticas más comunes son: malware; suplantación de identidad; *malware* en forma de correo no deseado; ataque de *ransomware*; violaciones de datos; y, el troyano y los riesgos/dificultades más comunes son: los ataques son cada vez más complejos; la dependencia de las empresas en hardware y software está creciendo; la creciente cantidad

de datos que necesita ser protegida y segura; La falta de desarrollo/capacitación es un desafío clave.

Por lo tanto, la ciberseguridad es ahora, y más que nunca, una prioridad para todos y cada país debe incluir algunas medidas y acciones relacionadas con este tema.

En las próximas dos secciones podemos ver las principales dificultades/barreras y algunas sugerencias/medidas/recomendaciones/mejores prácticas para mejorar la ciberseguridad.

5.2. Trabajo/Compañías

Las principales dificultades/barreras en los países involucrados en este informe con respecto a los trabajadores y la ciberseguridad son:

- Los ataques son cada vez más complejos y frecuentes y la principal motivación detrás de los ataques es la monetización;
- La seguridad en la nube se está convirtiendo en un problema crítico y se espera que las empresas dependan cada vez más de los proveedores de la nube;
- Las nuevas normas relativas a la protección de datos personales impondrán considerables demandas a las empresas;
- La importancia de las medidas organizativas (por ejemplo, gestión de riesgos) aumentará en el futuro en comparación con las medidas puramente técnicas;
- La dependencia de las empresas de productos de *hardware* y *software* representa una amenaza creciente;
- No hay suficientes incentivos para las inversiones en seguridad en las empresas;
- Falta de conciencia y estándares de seguridad;
- Todavía faltan fundamentos legales o son obsoletos en los países que dificultan la comprensión y la aplicación de medidas de seguridad;
- Falta de conciencia de seguridad por parte de la mayoría de las personas;
- Falta de personal capacitado/cualificado en seguridad cibernética y competencias digitales;
- Falta de actividades de capacitación para mejorar el conocimiento y un comportamiento mucho más seguro por parte de las personas;

- Falta de conocimiento de los empleados sobre las amenazas cibernéticas y las reglas de seguridad de TI;
- Falta de guías técnicas claras y concisas relacionadas con la ciberseguridad y la seguridad en Internet;
- El aumento de los requisitos salariales del personal cualificado en ciberseguridad puede complicar la situación;
- Muchas herramientas de seguridad separadas aumentan en última instancia la complejidad operativa y reducen la visibilidad de la postura general de seguridad;
- Las organizaciones a menudo no tienen un equipo formal de respuesta a incidentes de seguridad cibernética o incluso una persona nombrada responsable de lidiar con dicho incidente;
- Existe una falta de colaboración entre los equipos de privacidad y seguridad cibernética;
- Muchas compañías no tienen un plan de respuesta de ciberseguridad consistente;
- Falta de tiempo y recursos cualificados necesarios para implementar el plan de seguridad cibernética;
- Falta de un presupuesto adecuado para aumentar las capacidades de seguridad;
- *Hardware* y *software* de seguridad de TI obsoletos;
- Falta de compromiso por parte de la administración junto con un presupuesto insuficiente;
- Falta de participación entre todos los trabajadores en la estrategia de ciberseguridad (si existe);
- El inventario de activos con impacto en ciberseguridad no es bien conocido por todos los trabajadores de la empresa;
- La cultura de ciberseguridad necesita ser interiorizada, incluyendo programas y medidas de seguridad como procesos, gestión ambiental o de prevención de riesgos laborales;
- Pocas iniciativas centradas en la ciberseguridad industrial;
- No hay soluciones de ciberseguridad suficientemente probadas;
- Falta de cooperación entre la empresa y las iniciativas gubernamentales;

- Comunicación ineficiente entre los diferentes equipos debido a sus diferencias con respecto a sus conocimientos y capacidades sobre el uso de *software* y *hardware*;
- Hay actividades que pueden poner en peligro los sistemas y, como consecuencia, la seguridad de los procesos e instalaciones industriales;
- Falta de conocimiento de los efectos y la necesidad de nuevas tecnologías utilizadas para asegurar la interoperabilidad de los sistemas de control;
- Percepción general de que la amenaza es incierta y bastante improbable;
- El espionaje por medios digitales modernos amenaza la competitividad y la productividad nacional;
- Diferentes necesidades de ciberseguridad entre diferentes sectores de actividad;
- Falta de apoyo financiero para el desarrollo de la seguridad cibernética;
- Escasez o falta absoluta de estándares específicos para la seguridad cibernética;
- Malentendido del tema debido a la escasez de programas de capacitación enfocados y material de comunicación pública;
- Implementación incorrecta de soluciones y tecnologías de seguridad como firewalls, soluciones IDS/IPS, antivirus, etc.
- Ninguna relación o acuerdo entre autoridades, empresas y proveedores en relación con la ciberseguridad;
- Poca coordinación entre los diferentes estados miembros de la UE.

Para mejorar **la ciberseguridad en las empresas, propusimos algunas sugerencias/medidas/recomendaciones/buenas prácticas:**

- Proporcionar capacitación y sensibilización a todos los empleados en las actividades cotidianas;
- Las contraseñas siempre deben mantenerse en secreto y cumplir con una política predefinida. Además, la contraseña debe cambiarse regularmente;
- Utilice múltiples métodos de autenticación (por ejemplo, nombre de usuario/contraseña, respuesta a la pregunta de seguridad, certificado digital, tarjeta inteligente, huella digital, reconocimiento facial);

- En la configuración de un enrutador de LAN inalámbrica, es necesario establecer el estándar de cifrado WPA o WPA-2. Si la unidad no tiene una de estas configuraciones, se debe utilizar al menos el WEP estándar inseguro;
- Implementar más soluciones y tecnologías de seguridad como firewalls, soluciones IDS/IPS, antivirus, etc.
- Los programas antivirus y los cortafuegos deben mantenerse mediante actualizaciones periódicas. Esto también se aplica a todos los demás programas que se han instalado en una computadora para que se puedan cerrar las brechas de seguridad conocidas;
- No se deben utilizar soportes de datos externos (memorias USB, discos duros externos, DVD, etc.);
- Implementar una capacitación adecuada en los programas de pregrado y posgrado debe incluir temas relacionados con la seguridad cibernética para mejorar también la capacidad de recuperación de las instalaciones industriales existentes;
- Desarrollo de procedimientos y políticas para gestionar la ciberseguridad en entornos complejos interrelacionados;
- Creación de guías técnicas para mejorar el conocimiento de los trabajadores;
- Desarrollar métodos y sistemas para detectar funciones fallidas en redes internacionales;
- Desarrollar soluciones para el intercambio seguro de información para coordinar la respuesta a incidentes de ciberseguridad en el entorno de instalaciones industriales;
- Desarrollar técnicas para detectar, seguir y estudiar incidentes y cooperar con organizaciones de defensa;
- Desarrollar estrategias que mejoren los sistemas de información relacionados con la ciberseguridad;
- Desarrollo de estándares para varias áreas en el entorno de ciberseguridad industrial, tales como: equipos, interoperabilidad y gestión, recopilación y análisis de datos, pruebas y capacitación;
- Organizar eventos y talleres relacionados con la ciberseguridad para todas las partes interesadas e individuos;
- Acceda a sus recursos de intranet a través de la red privada virtual;

- Crear una estrategia de respuesta a incidentes;
- Implementar medidas para detectar compromisos y desarrollar un plan de respuesta a incidentes de seguridad cibernética;
- Formar un equipo de respuesta a la seguridad cibernética del incidente;
- Implementar un plan de riesgo de ciberseguridad en su empresa/organización y revíselo todos los años;
- Aumentar la conciencia sobre las amenazas cibernéticas en las empresas y cómo afectan el resultado final;
- La ciberseguridad debería ser responsabilidad de todos. Las organizaciones deben hacer de la ciberseguridad una parte central de la estrategia y cultura empresarial. Incrustado en la toma de decisiones estratégicas y se beneficia y adopta la innovación continua. Con respecto a este tema, ver por ejemplo: gestión del talento; cultura de riesgo y seguridad; y capacitación y concientización;
- Poner la ciberseguridad en el centro de la estrategia de una organización ayudará a mantener e incluso mejorar la confianza de los consumidores, los reguladores, los medios y otras partes interesadas relacionadas con las empresas/organizaciones;
- Desarrollar estrategias nacionales para ayudar a las empresas a tratar/responder a sus principales accidentes de ciberseguridad, si es posible para cada sector de actividad;
- Fomentar nuevas formas de asociación y participación de diferentes tipos de partes interesadas;
- Los programas utilizados en ordenadores y equipos tecnológicos siempre deben actualizarse con versiones recientes;
- Bloquear el acceso a sitios web malos y limitar el control de internet;
- Proteger la red Wi-Fi con una contraseña segura y una conexión con cifrado de datos y también cambiar la configuración predeterminada en el enrutador utilizado, cambiando la contraseña al panel de configuración del enrutador;
- Proporcionar capacitación a todos los trabajadores porque la mayoría de los trabajadores no tienen los conocimientos y competencias suficientes para tener un comportamiento seguro todo el tiempo;
- Tener copias de seguridad con todos los datos relevantes para el negocio;

- Involucrar a las personas en todas las iniciativas de tal manera que puedan contribuir con su experiencia y conocimiento;
- Desarrollar programas de habilitación, herramientas y técnicas y documentos de referencia que puedan respaldar el desempeño de los profesionales de seguridad cibernética;
- Organizar iniciativas de capacitación, manuales gratuitos y talleres que tengan en cuenta las diferentes necesidades;
- Las organizaciones deben realizar evaluaciones de riesgos periódicamente.

5.3. Vida privada

Las principales dificultades/barreras en su país con respecto a las personas y la ciberseguridad son las siguientes:

- Falta de conciencia y estándares de seguridad;
- Comportamientos negligentes al usar internet;
- Los programas actuales de las escuelas de pregrado no incluyen, la mayoría de las veces, temas de seguridad cibernética;
- Aunque existen buenas iniciativas, consejos y sugerencias, pero no llega a la población en general;
- Gran cantidad de *software* malicioso en el mercado;
- Comprensión inadecuada del estado del ciberataque;
- Hay muchas áreas rurales en las que no hay muchas ofertas de capacitación adicionales debido a la ubicación;
- La ayuda con dificultades generalmente solo está disponible por teléfono o en línea (con la excepción de ir directamente a la policía). Se necesita un punto de contacto directo, con el cual las personas también puedan contactar directamente en caso de problemas;
- Los reglamentos, políticas y leyes no están formulados de manera fácil para el usuario;
- La información sobre los materiales de apoyo a veces es muy difícil de encontrar (en Internet) y necesita un acceso más rápido y más fácil;

- Usar una contraseña débil, una contraseña para iniciar sesión en varias cuentas y no cambiar la contraseña;
- Falta de materiales de estudio sobre ciberseguridad;
- Las personas confían fácilmente en los archivos adjuntos de correo electrónico;
- Las personas comparten mucha información personal en las redes sociales;
- Falta general de interés de los jóvenes sobre la seguridad en Internet;
- Falta de conocimiento de las amenazas cibernéticas y las reglas de seguridad de TI;
- No hay muchas plataformas de ciberseguridad para intercambiar y compartir información;
- Falta de apoyo financiero para la promoción de la seguridad de Internet para las personas y el desarrollo de la ciberseguridad;
- Pocas iniciativas centradas en la seguridad de Internet en la vida cotidiana;
- Escasez de programas educativos y de capacitación y materiales públicos sobre seguridad en Internet;
- Baja alfabetización digital de los usuarios finales;
- Falta de conocimiento básico de amenazas potenciales de los usuarios públicos;
- No se ha creado una cultura de seguridad cibernética;
- Falta de guías técnicas claras y concisas sobre seguridad en Internet y seguridad cibernética;
- El inventario de activos con impacto en ciberseguridad no se conoce bien;
- Falta de conocimiento de los efectos y de la necesidad de nuevas tecnologías utilizadas para asegurar la interoperabilidad de los sistemas de seguridad/control;
- Malentendido de la seguridad cibernética y de Internet debido a la escasez de programas de capacitación enfocados y material de comunicación pública;
- Las políticas y procedimientos no son adecuados desde el punto de vista de la ciberseguridad;
- Los riesgos de ciberseguridad no están integrados en herramientas y sistemas;
- No hay soluciones de ciberseguridad suficientemente probadas;
- Implementación incorrecta de soluciones y tecnologías de seguridad como firewalls, soluciones IDS/IPS, antivirus, etc.

- Poca coordinación entre los diferentes estados miembros de la UE.

Para mejorar la seguridad cibernética de los ciudadanos en su vida privada, encuentre sugerencias/medidas/recomendaciones/buenas prácticas para mejorar a continuación:

- Usar una diversidad de protección para el ordenador, como protección antivirus, firewall y actualizaciones;
- No abrir archivos sospechosos, tener cuidado con los correos electrónicos bancarios y no hacer clic en ningún enlace;
- Las personas deben tener más cuidado con el software que se instalará (debido a malware, virus, ...);
- Prestar más atención a la información que se brinda durante las compras en línea, p. certificados y sellos, clasificaciones, protección al consumidor, "desconfianza saludable";
- Usar conexiones encriptadas;
- Las contraseñas deben tener, al menos, 8 caracteres y una combinación de letras mayúsculas y minúsculas, caracteres especiales, números y no reutilizarlos;
- Tener más cuidado con los sistemas de suscripción;
- Dar un buen ejemplo y hablar más sobre el uso del sistema y acuerdar las reglas;
- Mantener una copia de seguridad de todos sus datos;
- Implementar programas de capacitación y talleres sobre ciberseguridad para escuelas (pregrado y posgrado);
- La necesidad de revisar los currículos existentes en educación con respecto a estos temas;
- Desarrollar una plataforma educativa para mejorar el conocimiento de las personas sobre la seguridad de internet;
- Sensibilizar sobre las medidas y tecnologías de seguridad, como firewalls y antivirus;
- Crear guías generales para mejorar el conocimiento de las personas y que todos puedan entenderlas fácilmente con respecto a su educación y conocimiento;

- Implementar más soluciones y tecnologías de seguridad como firewalls, soluciones IDS/IPS, antivirus, etc.
- Organizar eventos y talleres relacionados con la ciberseguridad para todas las partes interesadas e individuos;
- Instalar versiones de *software* originales y actualizarlas cada vez que pueda.

6. Referencias

Ardielli, E., Ardiellli, J. (2017). Cyber security in public administration of the Czech Republic. Sociálně-ekonomická revue: VŠB-TUO. Retrieved from: https://fsev.tnuni.sk/revue/papers/147.pdf.

Bulletin Průmyslu 4.0. (2019). Národní centrum Průmyslu 4.0. Retrieved from: https://www.ncp40.cz/files/bulletin-prumyslu-2019-04.pdf.

Bundeskanzleramt, Digitales Österreich (2012). IKT-Sicherheit. Nationale IKT Sicherheitsstrategie Österreich. Wien: BM.I Digitalprintcenter.

Bundeskriminalamt (2015): Schutz vor IT-Kriminalität. Retrieved from: https://www.finkenstein.gv.at/_Resources/Persistent/94fb6a97ff9fafa801abe506dd7eb3cc5f6f6c31/IT-Sicherheit.pdf.

Bundeskriminalamt[1] (2019): IT-Sicherheit. Retrieved from: https://bundeskriminalamt.at/news.aspx?id=43534F5A38367453614D493D.

Bundeskriminalamt[2] (2019): IT-Sicherheit: 7 Tipps für Unternehmen und öffentliche Einrichtungen. Retrieved from: https://bundeskriminalamt.at/202/Internet_kennen/files/IT_Sicherheit_7_Tipps_fr_Unternehmen_Juni2015.pdf.

Bundesministerium für Inneres (2019): Schutz vor IT-Kriminalität. Retrieved from: https://www.bundeskriminalamt.at/202/Internet_kennen/files/TippsSchutzCybercrime_Juni2015.pdf.

Bundesministerium für Digitalisierung und Wirtschaftsstandort[1] (2019). Meldestellen. Retrieved from: https://www.onlinesicherheit.gv.at/erste_hilfe/meldestellen/249337.html.

Bundesministerium für Digitalisierung und Wirtschaftsstandort2 (2019). Informationssicherheit – Industrial Security. Retrieved from: https://www.usp.gv.at/Portal.Node/usp/public?gentics.rs=PDF&gentics.pb=notvisibleposition&contentId=10007.44661.

Busch, J./Soukup, A./Dutzler, H./Loinig, M./Gorholt, A. (2015). Industrie 4.0. Österreichs Industrie im Wandel. PwC Österreich GmbH Wirschaftsprüfungsgesellschaft.

CCI (2018). Spanish Industrial Cybersecurity Roadmap 2013 – 2018. Retrieved from https://www.cci-es.org/ documents/10694/0/Roadmap+CCI+English/998bbf3c-da70-4781-b40f-83d391f0cf85.

Centro Nacional de Cibersegurança Portugal (n.d.). Retrieved from: https://www.cncs.gov.pt/.

Cyber Sicherheit Steuerungsgruppe (2018). Bericht Cyber Sicherheit 2018. Wien: Cyber Sicherheit Steuerungsgruppe.

Cyber Sicherheit Steuerungsgruppe (2019). Bericht Cyber Sicherheit 2019. Wien: Cyber Sicherheit Steuerungsgruppe.

Delloite (2017). Industry 4.0 and cybersecurity - Managing risk in an age of connected production. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiFubazxb7jAhUVolwKHUbTA7oQFjAAegQIAxAB&url=https%3A%2F%2Fwww2.deloitte.com%2Finsights%2Fus%2Fen%2Ffocus%2Findustry-4-0%2Fcybersecurity-managing-risk-in-age-of-connected-production.html&usg=AOvVaw0mfdMLmiERC-Aec8s71G2s.

Delloite (n.d.) Indústria 4.0. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwi15be5x77jAhXXAmMBHanIAvsQFjACegQIARAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fpt%2FDocuments%2Ftransportation-infrastructures-services%2Findustria4_0medidas-pt.pdf&usg=AOvVaw1WbNQpRq0JufT1IYQvw5x0.

EY (2018). Is cybersecurity about more than protection? EY Global Information Security 2018-19. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiEhdODx77jAhUZ8uAKHUcxCGIQFjAAegQIBRAB&url=https%3A%2F%2Fwww.ey.com%2Fen_gl%2Fadvisory%2Fglobal-information-security-survey-2018-2019&usg=AOvVaw2H0YlwJ2GWhy7IEPTTLYMS.

EY (n.d.) Cybersecurity for Industry 4.0 - Cybersecurity implications for government, industry and homeland security. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjWlevexb7jAhWLQUEAHTANCa4QFjAAegQIBBAC&url=https%3A%2F%2Fwww.ey.com%2FPublication%2FvwLUAssets%2Fey-cybersecurity-for-industry-4-0%2F%24File%2Fey-cybersecurity-for-industry-4-0.pdf&usg=AOvVaw3Na4d6orEYCSgwo3f3q3Ku.

EY (2018). Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017-18. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwid7Mv66ZPjAhX1QEEAHZQ-AQkQFjAAegQIABAC&url=https%3A%2F%2Fwww.ey.com%2FPublication%2FvwLUAssets%2Fey-cybersecurity-regained-preparing-to-face-cyber-attacks%2F%24FILE%2Fey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf&usg=AOvVaw0wrAdSeBMKqIg9uxX4YEC9.

Gabinete de Estratégia e Estudos (2018). A Cibersegurança em Portugal. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjNnMPwx77jAhUK-hQKHSLWDY0QFjABegQIBRAC&url=https%3A%2F%2Fwww.gee.gov.pt%2F%3Foption%3Dcom_fileman%26view%3Dfile%26routed%3D1%26name%3DTE56%2520-%2520A%2520Ciberseguran%25C3%25A7a%2520em%2520Portugal.pdf%26folder%3Destudos-e-seminarios%2Ftemas-economicos%26container%3Dfileman-files&usg=AOvVaw1CGUQIIQs7DHKQDX0E5Y-s.

Gabinete de Estratégia e Estudos (2019). Ponto de Situação da Cibersegurança em Portugal. Retrieved from: https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=imgres&cd=&ved=2ahUKEwjt3-ayzr7jAhULnhQKHaMGDGYQ5TV6BAgBEAg&url=https%3A%2F%2Fwww.gee.gov.pt%2F%3Foption%3Dcom_fileman%26view%3Dfile%26routed%3D1%26name%3DPowerPoint%2520GEE%2520-%2520Coimbra%2520(ENIAP)%25202019-01-26%2520GOB.pdf%26folder%3Destudos-e-seminarios%252Fparticipacao-em-conferencias%252F2019-3%26container%3Dfileman-files&psig=AOvVaw25PWkebk5Fiznu9PuAPFzu&ust=1563544257946449.

Federal Chancellery of the Republic of Austria (2013). Austrian Cyber Security Strategy. Wien.

Fernández, L. España y la ciberseguridad: hora de remangarse. Revista SIC,410, 27-37. Retrieved from https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomia Industrial/410/LUIS%20FERN%C3%81NDEZ%20DELGADO.pdf.

Gmv Innovation Solutions (n.d.) Cibersegurança. Retrieved from: https://www.gmv.com/pt/Sectores/SegurancaInformacao/.

Iniciativa Průmysl 4.0 (2015). Ministerstvo průmyslu a obchodu. Retrieved from: https://www.mpo.cz/assets/dokumenty/53723/64358/658713/priloha001.pdf

Kaspersky Lab. (2019). Span and phishing in 2012. Retrieved from: https://securelist.com/spam-and-phishing-in-2018/89701/.

Microsoft (n.d.). Trends in Global Cybersecurity. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwiy1tfUyb7jAhVlA2MBHagjB6QQFjAFegQIABAC&url=https%3A%2F%2Finfo.microsoft.com%2Frs%2F157-GQE-382%2Fimages%2FEN-US-CNTNT-eBook-Security-Trends-In-Global-Cybersecurity.pdf&usg=AOvVaw04gc_UHooXgmmdPcO-c-Vx.

Microsoft (2018). Microsoft Security Intelligence Report Volume 23. Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwiy1tfUyb7jAhVlA2MBHagjB6QQFjACegQIBRAC&url=https%3A%2F%2Finfo.microsoft.com%2Frs%2F157-gqe-382%2Fimages%2Fen-us_cntnt-ebook-sir-volume-23_march2018.pdf&usg=AOvVaw0OJ4NbRtj5pdkCoWxfQjVP.

Ministerio del Interior España (2017). Estudio sobre la Cibercriminalidad en España. Secretaría de Estado de Seguridad. Retrieved from http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70.

Modern massive Data Analysis for Industry 4.0 Industry 4.0 at VŠB-TUO (2016). Faculty of Electrical Engineering and Computer Science VŠB-TUO Czech Republic. Retrieved from: https://www.czelo.cz/files/prezentace-pozvanky/1-Snasel-2016-e-mail.pdf.

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 (2015). Národní bezpečnostní úřad. Retrieved from: https://www.cybersecurity.cz/data/navratil2014.pdf.

Nic.at GmbH (2018). Bericht Internet-Sicherheit Österreich 2017. Wien: nic.at GmbH.

OECD (2017). Digital Economy Outlook 2017. Retrieved from: https://www.oecd.org/internet/oecd-digital-economy-outlook-2017-9789264276284-en.htm.

PwC (n.d.). Industry 4.0: Global Digital Operations Study 2018. Retrieved from: https://www.strategyand.pwc.com/industry4-0.

Pwc (2018). Global Digital Operations 2018 Survey. https://www.strategyand.pwc.com/industry4-0#Download.

Safer Internet (2019). Ministerstvo vnitra České republiky. Retrieved from: https://www.mvcr.cz/clanek/safer-internet.aspx.

Security Strategy of the Czech Republic (2015). Ministry of Foreign Affairs of the Czech Republic. Retrieved from: http://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf.

Simio (n.d.). Industry 4.0. Retrieved from: www.simio.com/applications/industry-40.

Spanish Government (2017). National Security Strategy. Government Presidency. Retrieved from https://www.dsn.gob.es/sites/dsn/files/2017_Spanish_National_Security_Strategy_0.pdf

Spanish Government - CCN-CERT (2018). Cyber threats and trends 2018. National Cryptologic Centre. Retrieved from https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2997-ccn-cert-ia-09-18-cyberthreats- and-tendencies-executive-summary-2018-1/file.html.

Spanish Government - CCN-CERT (2019). Aproximación española a la Ciberseguridad. Centro Criptológico Nacional. Retrieved from https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/16-decalogo-ciberseguridad-2018/file.

Spanish Government - CCN-CERT (2019). Ciberamenazas y tendencias 2019. Centro Criptológico Nacional. Retrieved from https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html.

Spanish Government - INCIBE (2015). Gestión de riesgos, una guía de aproximación para el empresario. Retrieved from https://www.incibe.es/protege-tu-empresa/blog/gestion-riesgos-seguridad-informacion.

Spanish Government - INCIBE (2016). Market Trends in Cybersecurity. Spanish National Cybersecurity Institute. Retrieved from https://www.incibe.es/sites/default/files/estudios/cybersecurity_market_trends.pdf.

Spanish Government - INCIBE (2017). Decálogo de ciberseguridad empresas. Una guía de aproximación para el empresario. Retrieved from https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf.

Spanish Government - INCIBE (2018). La ciberseguridad es cosa de todos, establece buenas prácticas. Retrieved from https://www.incibe.es/protege-tu-empresa/blog/ciberseguridad-cosa-todos-establece-buenas-practicas.

Strategie kybernetické obrany ČR (2018). Národní centrum kybernetických operací. Retrieved from: http://www.acr.army.cz/assets/informacni-servis/zpravodajstvi/strategie-kyberneticke-obrany.pdf.

Sevillano, F. (2019). Principales incidentes de ciberseguridad en España durante 2018. Retrieved from https://willistowerswatsonupdate.es/ciberseguridad/ciberataques-en-espana-2018/.

The Czech Republic opened national cyber security center (2019). National Cyber Security Center. Retrieved from: https://www.govcert.cz/en/info/events/2456-the-czech-republic-opened-national-cyber-security-center/.

Verein Industrie 4.0 (2016). Österreichischer Normungs-Kompass Industrie 4.0. Retrieved from: https://plattformindustrie40.at/wp-content/uploads/2016/12/WEB_INDUSTRIE_4.0_ES-2.pdf.

WebsiteBuilderExpert (2018). Which EU Country is Most Vulnerable to Cybercrime. Retrieved from: https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/.

Wirtschaftskammer Steiermark (2019). Cyber-security-hotline. Retrieved from: https://www.wko.at/Content.Node/kampagnen/cyber-security-hotline/index.html#unternehmen.

WKO Bundessparte Information und Consulting (2019). IT-Sicherheitshandbuch für KMU. Retrieved from: https://www.wko.at/site/it-safe/sicherheitshandbuch.html.

World Economic Forum (2019). The Global Risks Report 2019. Retrieved from: https://www.weforum.org/reports/the-global-risks-report-2019.