EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

Nº 72

junio 2020

Boletín divulgativo de Innovación y Nuevas Tecnologías
Publicado por el Gabinete Tecnológico
Dirección de Tecnologías de la Información y la Comunicación

ÍNDICE

En el primer artículo de este nuevo ejemplar del boletín Aurrera os presentamos un nuevo concepto que actualmente está en auge en muchas empresas, y que recibe el nombre de *«RPA: Automatización robótica de procesos»*. Como veremos en el artículo, puede ser una buena herramienta para que las empresas digitalicen muchos de sus procesos.

En el segundo de los artículos, titulado *«Evolución del modelo de ciberseguridad del Gobierno Vasco y su sector público»*, analizamos el presente y, sobre todo, el futuro del modelo de ciberseguridad del Gobierno Vasco para hacer frente a las amenazas que nos acechan todos los días en Internet.

Continuando con los consejos sobre Windows10 y Office365 que se están implantando en los puestos corporativos del Gobierno Vasco, en esta ocasión nos centramos en uno de los productos que incorpora el nuevo Office 365, se trata en concreto de «Teams». Una utilidad que ha permitido a muchas personas desde sus domicilios particulares seguir en contacto con sus compañeros/as durante la crisis sanitaria provocada por el coronavirus Covid-19, y que poco a poco iremos usando cada vez más incluso desde nuestro puesto de trabajo.

En la contraportada, os presentamos «Ni.eus», el nuevo servicio de email en euskera que ha puesto en marcha recientemente la Fundación PuntuEUS y que va dirigido especialmente a personas «euskaldunes» que hagan uso de Internet, particulares, asociaciones y empresas.

Durante los últimos meses, el coronavirus Covid-19 se ha hecho famoso y desgraciadamente ha marcado la vida de millones de personas en todo el mundo. Sin embargo, y en contra de lo que muchas personas piensan, los coronavirus no son nuevos, ya que fueron descubiertos en 1967 por June Almeida. En el apartado *«Protagonistas»* hacemos un breve repaso a la vida de esta científica escocesa que gracias a la tecnología desarrolló un método para mejorar la visualización de los virus.

RPA: Automatización robótica de procesos

La automatización robótica de procesos es, actualmente, junto a la Inteligencia Artificial y al Big Data, una de las piezas clave que están usando las empresas para llevar a cabo su «transformación digital».

[1] **RPA:** son las siglas en inglés de *«Robotic Process Automation»* (en castellano, «Automatización Robótica de Procesos»).

Este nuevo tipo de soluciones tecnológicas utilizan lo que se llama «robots de software» e inteligencia artificial (IA) para gestionar procesos.

En muchas ocasiones, las tareas que realizamos en el trabajo son repetitivas y monótonas, y normalmente las personas aportan poco valor añadido a las mismas.

En las fábricas, cuando el trabajo consiste en realizar grandes esfuerzos físicos o precisamente tareas repetitivas, se suelen utilizar máquinas o robots. Pues bien, esa misma filosofía es la que se aplica ahora al mundo no físico, es decir, al de los **procesos**, con la única diferencia que, en este caso, se habla de RPA[1] o *«automatización robótica de procesos»*.

Veamos en qué consiste exactamente.

RPA

Las empresas llevan utilizando software de automatización desde hace muchos años. Sin embargo, es ahora cuando esta tecnología está más en auge que nunca en muchas empresas y sectores.

El robot (o bot) que se instala, y que consiste en un **software**, interactúa con los sistemas de la misma manera que lo haría una persona, pulsa unos botones, rellena un formulario o lee el contenido de un documento, por ejemplo. De todas formas, si instalamos un RPA en nuestra empresa, no veremos a un robot sentado en nuestra silla, ya que funcionará como lo hace otra aplicación o software.

La automatización de procesos tiene como objetivo optimizar el tiempo de ejecución de aquellas tareas que son repetitivas, monótonas, complejas y que normalmente las hacemos las personas de forma manual. Gracias a ello se logra dos cosas: reducir el tiempo de respuesta y minimizar los errores causados por la fatiga.

Algunas de las tareas más habituales que hoy en día se están automatizando son:

- ✓ Gestionar y cumplimentar formularios con datos que ya tenemos archivados
- ✓ Buscar, crear, actualizar o eliminar registros de una base de datos
- ✓ Elaborar informes que tengan una estructura predefinida

- ✓ Generar informes que requieran cálculos y validaciones
- ✓ Monitorizar transferencias

A día de hoy, los «robots de software» son capaces de trabajar con cualquier tipo de

aplicación informática, desde una simple hoja de cálculo, hasta una aplicación web, incluso con sistemas Cliente/Servidor.

PRIMEROS PASOS

Muchas personas piensan que automatizar un proceso consiste únicamente en instalar un software. Cuando, en realidad, supone realizar un trabajo previo de análisis y elección de los procesos que se quieren automatizar y, posteriormente, definir la ejecución, mantenimiento y seguimiento de los procesos.

El primer paso consiste en definir el diagrama de los **procesos** a automatizar y, a continuación, las **actividades** y las **tareas** que lo componen (detallando los **roles** de las personas responsables que intervienen). Después debemos establecer cuáles son las **aplicaciones** que se utilizan en cada una de las tareas antes definidas, de tal manera que podamos establecer qué tipo de interacción tendrá con el RPA (por ejemplo, accesos y demás configuraciones necesarias para los robots).

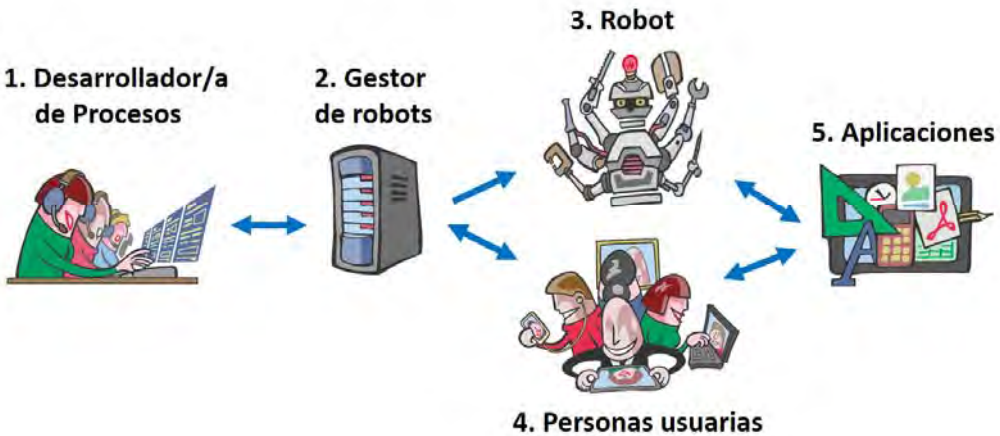
Una vez que tenemos definida la capa de procesos + actividades + tareas (así como las aplicaciones), podemos diseñar la capa de los **robots**.

En el mercado existen aplicaciones, por ejemplo basadas en *«low-code»*[2], que facilitan a las empresas diseñar y mantener los robots de software.

El siguiente paso consiste en que la empresa reorganice su estructura tecnológica y sus recursos humanos (en este caso, modificando el rol de algunos puestos y creando otros nuevos).

Las piezas que componen el puzzle de un RPA son básicamente:

1. Los **desarrolladores**: son las personas encargadas de identificar las tareas o procesos que va a desarrollar el RPA.
2. El **gestor de robots**: es la parte encargada de asignar y monitorizar las tareas.
3. El **robot de software**: es el encargado de interactuar directamente con las aplicaciones de negocio y hacer el trabajo.
4. Las **personas**: se encargarán de resolver las incidencias (o excepciones) que el robot no pueda tramitar.



Esquema basado en el informe «Automatización Robótica de Procesos (RPA)» [2017] de Deloitte

5. La **aplicación**: es el programa o plataforma a través de la cual el robot interactúa con las personas usuarias.

BENEFICIOS

La automatización robótica de procesos aporta beneficios tanto a las empresas como a las personas que hacen el trabajo que se quiere automatizar, siendo los más

[2] **Low-Code:** se trata de una serie de plataformas con las que se pueden desarrollar aplicaciones reduciendo al mínimo el desarrollo de código de forma manual. Normalmente, se utiliza una interfaz visual, utilidades *«drag and drop»* (arrastrar y soltar) y componentes preconfigurados. Precisamente, gracias a ello, personas con pocos conocimientos técnicos en temas TIC pueden desarrollar y desplegar aplicaciones empresariales con cierta facilidad.

El término *«Low-Code»* fue utilizado por primera vez en 2014 en un informe de la empresa Forrester redactado por los analistas Clay Richardson y John Rymer.

significativos los siguientes:

- **Costes**: las tareas manuales y repetitivas que realiza una persona, a partir de ahora serán gestionadas por el software RPA y, por lo tanto, se reduce el coste de su gestión.
- **Tiempo**: el trabajo se hace en menos tiempo, y las personas se pueden dedicar a otras labores.
- **Calidad**: la automatización reduce significativamente el número de errores, y ello implica que al final se obtiene un mejor servicio.
- **Flexibilidad**: si por algún motivo los procesos de negocio cambian, es suficiente con rediseñar (actualizar) las reglas del RPA y reconfigurar el bot, lo cual se puede hacer en poco tiempo.
- **Seguimiento**: se pueden hacer mediciones online para establecer mejoras continuas en los procesos que se han definido.
- **Digitalización**: los RPAs no procesan tareas que están en formato papel. Por lo que, todas las tareas o procesos que se quieran automatizar, tienen que hacerse sobre documentos digitalizados. Por lo tanto, y aunque sea de forma indirecta, los RPAs impulsan la digitalización de muchos procesos.

CRITERIOS

En el mercado existen distintos tipos de robots[3], por eso es importante tener claro los criterios en los deberíamos fijarnos a la hora de elegir un RPA u otro:

- ✓ **Arquitectura**: en primer lugar, es importante conocer cómo se estructura la herramienta, ya que en función de ello se podrán crear diseños más o menos complejos.
- ✓ **Usabilidad**: la facilidad de uso es siempre un tema a tener en cuenta, ya que en función de ello será más fácil su implantación y que las personas puedan sacarle un mayor provecho.
- ✓ **Integración**: es importante conocer la capacidad que tiene el RPA para relacionarse con otros sistemas y otras tecnologías, ya que para realizar su trabajo debe interactuar con distintos sistemas.
- ✓ **Excepciones**: otro aspecto que en muchas ocasiones suele pasar desapercibido, es la capacidad que ofrece el RPA para manejar excepciones de negocio, y en las que se requiere una actividad manual por parte de una persona.
- ✓ **Seguridad**: el RPA deberá disponer de una buena gestión de accesos y roles. Cada persona, equipo o departamento debe tener sólo los permisos que

[3] **Tipos de bots:**

Robots de front office: se encargan de los procesos enfocados al exterior, como pueden ser los relacionado con las ventas o la atención al cliente. En estos procesos siempre habrá personas para tomar decisiones que requieran un criterio humano.

Por ejemplo, un *«call center»* puede usar un RPA como asistente. Los empleados/as del call center acceden a múltiples sistemas online para conocer el historial del cliente, el estado actual del pedido, etc.

Robots de Back office: son los procesos desatendidos o de *«background»* que dan soporte al funcionamiento de la empresa.

Incluyen tareas como transferencias de archivos, generación de informes o sistemas de monitorización. Se suelen lanzar fuera del horario de oficina para no saturar los sistemas.

Por ejemplo: los datos recopilados durante las transacciones con el cliente pueden volcarse automáticamente en un informe y después se comparte (a través de un correo electrónico) con otra persona.

RaaS

Uno de los conceptos que ya se ha hecho habitual en el mundo de las Nuevas Tecnologías son las siglas «SaaS», que hacen referencia al *«Software as a Service»*, y que engloba a las aplicaciones que están instaladas en la nube para que las empresas que las necesiten las puedan usar cuando les sea necesario (normalmente ese servicio se suele contratar mediante una suscripción). Pues bien, de forma análoga se ha creado otro acrónimo, para la automatización robótica, cuyas siglas son «RaaS» (*«Robot as a Service»* o *«Robotics as a Service»*).

Por lo tanto, la automatización robótica también se puede implementar en la nube y ofrecer a las empresas aquellas aplicaciones de automatización necesarias, a las que se accederá como un servicio más.

Un ejemplo típico de esta modalidad es el uso que hacen las tiendas o almacenes de ropa, por ejemplo, para realizar la gestión automática de su stock.

realmente necesite (por ejemplo: unas personas deberán poder editar un flujo de trabajo, mientras que otras sólo deberían poder verlo). Además, sería conveniente que ofreciese un registro de las acciones que lleva a cabo cada persona.

«Aunque sea de forma indirecta, los RPAs impulsan la digitalización de muchos procesos»

- ✓ **Configuración**: es importante que un RPA incluya la opción de monitorizar y gestionar los procesos automatizados desde una consola central. Ello permitirá realizar el seguimiento de las operaciones e identificar problemas que puedan surgir.
- ✓ **Implementación**: debemos analizar detenidamente las funciones que ofrece la nueva plataforma para ser implementado en un Entorno de Producción, lo cual incluye tareas como distribuir versiones entre máquinas, personalizar las variables del entorno, proporcionar controles de seguridad, etc.
- ✓ **Soporte**: otro aspecto importante es disponer de un buen proveedor[4], un buen soporte y una buena documentación, sin olvidarnos de la formación que hay que dar a las personas que van a utilizar el software.

A la hora de automatizar procesos es conveniente pensar en el futuro, y analizar también cómo se podría expandir el RPA a otras áreas de la empresa a medida que vaya creciendo nuestro negocio, ya que si nos centramos en automatizar procesos individuales (de forma aislada) seguramente tendremos problemas en el futuro para expandir el RPA.

SECTORES

Los RPAs se van extendiendo poco a poco y, a día de hoy, los sectores en los que más éxito están teniendo son los relacionados con la **manufacturación**, las fábricas de **montaje** y el sector de la **salud** (farmacéuticas…).

Otro sector en el que están en auge los RPAs es el de los **servicios telefónicos** de atención al cliente. Por ejemplo, muchas empresas usan los robots de chat inteligentes para simular una conversación humana y resolver las incidencias de sus clientes.

Otro sector es el de los **seguros**. Las empresas aseguradoras normalmente manejan una gran cantidad de documentos y flujos de trabajo. En estos casos, los robots gestionan casi todas las etapas de una reclamación: recepción de la propia queja, descarga y verificación de los datos enviados y el cálculo del pago (las personas sólo intervienen a la hora de chequear las excepciones que requieren de un criterio humano).

Las **empresas tecnológicas** también están empezando a usar cada vez más los robots. Un ejemplo muy habitual es la solicitud para restablecer la contraseña de una persona. En estos casos, el robot recibe la solicitud, analiza la tarea que hay que

realizar (que puede estar basada en unas reglas), y a continuación restablece la contraseña de la persona que lo ha solicitado, sin necesidad de que intervenga una persona en todo el proceso. Otras organizaciones usan los bots, por ejemplo, para crear VPNs, etc.

Otro sector importante es el de las **entidades financieras**. Los procesos automatizados en los bancos permiten hoy en día evaluar de forma más eficaz los datos necesarios para tomar ciertas decisiones. Por ejemplo, a la hora de calcular la solvencia de un cliente, conceder o no un crédito, etc. ❑

[4] **Proveedores:** relación de algunos proveedores de RPAs:

- Automation Anywhere
- Blue Prism
- HelpSystems
- Kryon Systems
- Kofax
- NICE
- Pegasystems
- Redwood
- UiPath
- WorkFusion
- …

Evolución del modelo de ciberseguridad del Gobierno Vasco y su sector público

Los peligros que nos acechan en Internet son cada vez más sofisticados, por lo que conviene estar bien preparados.

El contexto de las amenazas que nos acechan en Internet se ha diversificado, siendo cada vez más complejo y variado, donde existen redes criminales que cuentan con abundantes recursos y motivaciones diversas.

Los agentes o motivaciones más habituales suelen ser Redes Criminales, «Hacktivistas», Ciberespionaje o Ciberterrorismo, y las características principales son:

- ✓ Ataques cada vez más dirigidos
- ✓ Facilidad de acción -> Económico
- ✓ Compleja jurisdicción -> Impunidad
- ✓ Dispersión de la motivación

La continua evolución de las amenazas requiere un enfoque más amplio en materia de ciberseguridad. Por este motivo, las organizaciones deben mejorar sus capacidades incorporando otras nuevas.

Como muestra, el pasado año hubo un ataque cibernético a una entidad pública vasca realizado por Ciberdelincuentes —en este caso, una banda organizada de Europa del Este, lo que conlleva una alta impunidad— el cuál provocó un grave impacto en los servicios que presta la entidad atacada.

El ataque fue relativamente fácil de desplegar, altamente exitoso y persistente en el tiempo. Normalmente, estos ataques se introducen en las organizaciones a través de vulnerabilidades de los sistemas o mediante engaños (ingeniería social[5]). Recogen o ex filtran datos que les permita ampliar el radio de afección o hacerse con información relevante; y pueden estar meses «dormidos» hasta que se activan y provocan la indisponibilidad de los activos infectados (ordenadores, servidores...). En ese momento, se exige a la empresa un rescate en criptomonedas para su liberación.

Este ataque, en concreto, se realizó dentro de una campaña orquestada a nivel mundial y que tuvo una importante afección en Euskadi.

«El "Plan Director de Seguridad" tiene como objetivo marcar el camino de BATERA en materia de Ciberseguridad para los próximos 4 años»

Como resultado, han provocado la indisponibilidad de los servicios informáticos y fugas de información. La recuperación de los activos ha sido muy compleja y lenta, con un coste económico elevado.

LECCIONES APRENDIDAS Y NUEVOS RETOS

De todas estas situaciones es importante aprender las lecciones que nos dejan y preparar el futuro. Por lo tanto, debemos atender estos nuevos retos que nos plantea la ciberseguridad:

1. **Ampliar el ámbito de actuación** («salir del perímetro»). Hoy en día las principales amenazas están en el ciberespacio, lo que nos obliga a estudiar y aprender del comportamiento de los/as atacantes. Es

[5] **Ingeniería social:** (en inglés *«Social Engineering»*) incluye todos aquellos engaños y demás técnicas utilizadas por un/a pirata informático/a para sacar información a una persona sin que ésta se dé cuenta de que esta revelando «información sensible» (por ejemplo, una contraseña) o bien conseguir que una persona realice una acción concreta (por ejemplo, abrir un archivo que contenga un virus).
Para más información, podéis consultar el artículo titulado *«Ingeniería social»*, publicado en el boletín Aurrera nº 13 (marzo de 2004).

necesario hacer seguimiento y monitorización de nuestros activos de información más allá de nuestros sistemas de información.

2. **Reforzar mecanismos de investigación e inteligencia**. La constante evolución y sofisticación de las ciberamenazas requiere un fortalecimiento de los mecanismos predictivos de detección y análisis de amenazas.
3. **Fortalecer la disuasión**. Reforzar la resiliencia de las organizaciones. Ampliar las capacidades de prevención, detección y respuesta de nuestros sistemas de información. Anticipar y acortar los tiempos de actuación. Mejorar los mecanismos de vigilancia y aplicación de medidas de contención.
4. **Entrenamiento y concienciación**. Fomentar la realización de ciberejercicios y evaluaciones de seguridad entre el personal de nuestra organización. En definitiva, incrementar las campañas de concienciación y formación.
5. **Ampliar la capacidad de respuesta ante incidentes**. Es necesario orquestar un tratamiento de gestión de incidentes que posibilite una respuesta robusta. Es conveniente que articule elementos de colaboración externo para apoyo a la recuperación y, además, que establezca medidas de cooperación judicial y policial.
6. **Aplicar la seguridad en el Diseño**. Proponer requerimientos de seguridad como requerimientos de negocio. Establecer mecanismos de revisión y medición de dichos requisitos. Incorporar más seguridad a los servicios BATERA[6] (Infraestructuras, Backup, Puesto, Aplicaciones críticas para la misión y la vida).
7. **Alinear el Marco Regulatorio** con el Marco Operativo. ENS, ISO 27000, ISO 22301.

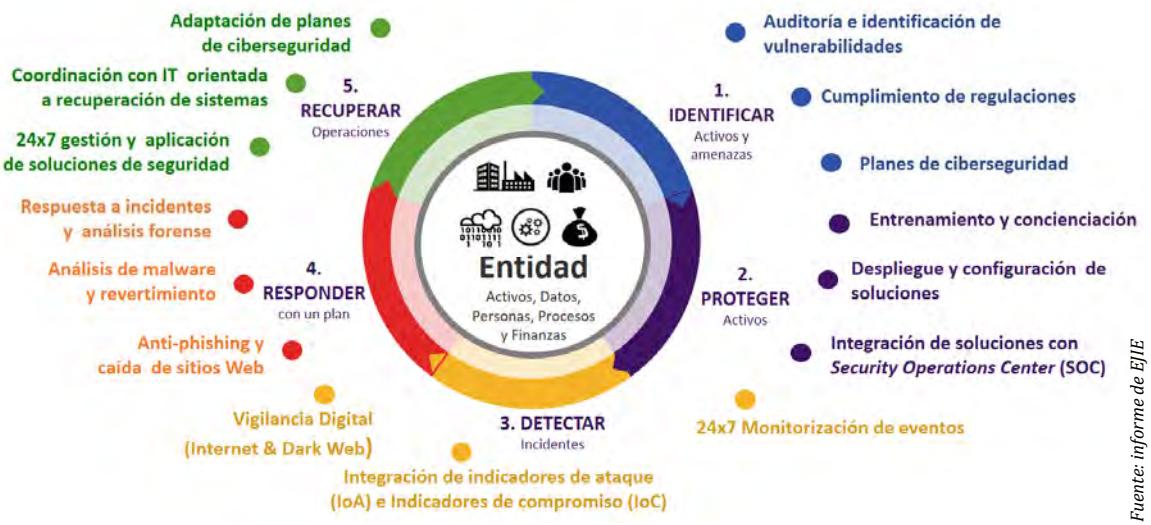
Y, por supuesto, mantener y reforzar los servicios tradicionales de protección y soporte a la seguridad y lucha con los sistemas obsoletos.

ENFOQUE OPERATIVO

Los principales servicios que actúan como soporte de seguridad IT en BATERA están recogidos en un **Marco Regulatorio y de Gobierno de Seguridad IT**.

Los principales componentes de este marco son:

1. Una Oficina Técnica de Seguridad, en EJIE, para el cumplimiento del RGPD, el ENS, las Infraestructuras críticas y los Servicios esenciales y servicios digitales, así como para el cumplimiento del SGSI bajo norma ISO 27001 y la consultoría en continuidad de negocio.
2. Un *«Security Operation Center»*, encargado de la monitorización de eventos de seguridad, de la gestión y evolución del sistema de control, de la colaboración en la resolución de incidentes de seguridad, del análisis de vulnerabilidades, de las auditorías de seguridad y de las auditorias de concienciación y formación.



Fuente: informe de EJIE

[6] **BATERA:**

El **27 de julio de 2015** el Consejo de Gobierno aprobaba la *«Propuesta de Acuerdo del Consejo de Gobierno en relación con el proceso de Convergencia en materia de Tecnologías de la Información y la Comunicación»*, es decir, la puesta en marcha de «BATERA», el proceso de convergencia que establece el modelo de gestión TIC para el sector público de la Comunidad Autónoma de Euskadi (CAE).

Posteriormente, el Consejo de Gobierno de **21 de junio de 2016** adoptó el Acuerdo presentado como *«Propuesta de Acuerdo relativa al proceso de Convergencia en materia de Tecnologías de la Información y la Comunicación»* que aprueba el documento ejecutivo y autoriza la implementación del proceso de convergencia según el plan general de actuación presentado.

Batera

3. Una Gestión de Plataformas de Seguridad, para la operación de infraestructuras de seguridad, el tratamiento de las incidencias de seguridad de las actualizaciones de seguridad, del parcheado y bastionado de servicios y de la gestión de «Backups».
4. Un CSIRT[7], como Centro de respuesta a incidentes para realizar alertas tempranas, el análisis forense, la interlocución con otros CERTs[8] y la gestión de crisis.
5. Un servicio de Evolución Tecnológica, con participación en implantaciones de proyectos de seguridad, evaluación de nuevas tecnologías de seguridad, la interlocución con el resto de oficinas técnicas, y el apoyo al CISO[9].

[7] **CSIRT**: son las siglas de «Equipo de Respuesta ante Emergencias Informáticas»

[8] **CERT:** son las siglas de «Centro de Respuesta a Incidentes de Seguridad para ciudadanos y empresas»

[9] **CISO:** son las siglas de Director/a de Seguridad de la Información

[10] **MITRE ATT&CK**: (Tácticas, Técnicas y Conocimiento Común de Adversarios). Es una manera de describir y categorizar los comportamientos adversos basados en las observaciones de todo el mundo. Es decir, es una lista estructurada de comportamientos conocidos de los/as atacantes que se recopilaron en tácticas y técnicas y se expresaron en unas matrices. Esta lista es una representación integral de los comportamientos que los atacantes usan cuando ponen en peligro las redes, y es útil para una variedad de medidas, representaciones y otros mecanismos ofensivos y defensivos.

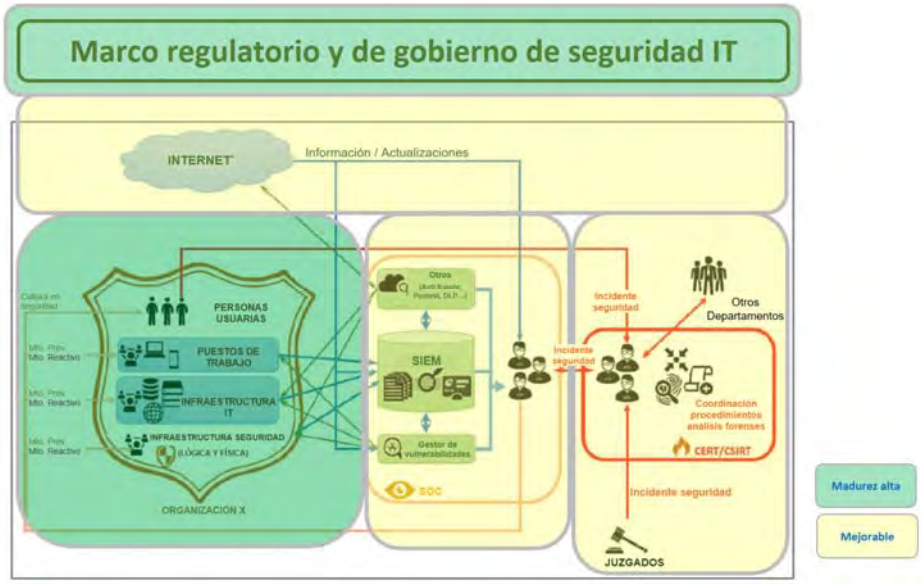
Actualmente, la madurez de los servicios de soporte de BATERA es alta, como demuestra el hecho de que, a pesar de recibir ataques de forma habitual, los mismos no han tenido un impacto relevante. Sin embargo, el riesgo se acrecienta y se evidencia la necesidad de reforzar la seguridad.

NUEVOS SERVICIOS DE SEGURIDAD

A continuación, se analizan y presentan los aspectos más relevantes relacionados con los nuevos servicios de seguridad que se quieren ofrecer en BATERA de manera prioritaria.

Tal y como ya hemos indicado, el contexto actual en materia de Ciberseguridad resulta cada vez más complejo. En un entorno en el que la movilidad y, en consecuencia, los servicios en «cloud» y el nivel de exposición de los servicios internos es creciente, el **nivel de riesgo** aumenta proporcionalmente. Por su parte, las redes criminales están cada vez más especializadas y tienden a dirigir y elaborar cada vez más sus ataques, con objeto de obtener un retorno de la «inversión» que realizan.

Por ello, este contexto requiere un enfoque más amplio en materia de Ciberseguridad, motivo por el cual EJIE, dentro del proyecto BATERA, se encuentra en una fase de



Fuente: informe de EJIE

«Evolución de los Servicios de Seguridad» que ofrece actualmente de cara a mejorar las capacidades ya disponibles y a la incorporación de nuevas capacidades y funcionalidades que permitan hacer frente a las amenazas de la situación actual.

Como punto de partida de esta fase de evolución, se está realizando un «Plan de Evolución de Servicios de Seguridad» o «Plan Director de Seguridad» que pretende marcar el camino de BATERA en materia de Ciberseguridad para los próximos 4 años. Para llevar a cabo dicho Plan se utilizarán referencias internacionales en el modelado de la seguridad, como puede ser el «NIST Cyber Security Framework» o la matriz «MITRE ATT&CK»[10].

Aunque el Plan no está finalizado, se han identificado una serie de necesidades que hay

que acometer de manera prioritaria, y son las siguientes:

1. Evolución del **Servicio de Backup**: Ante cualquier ataque de seguridad que comprometa los servicios IT que presta EJIE, las copias de seguridad son el último recurso que garantiza poder restablecer el servicio. Por lo tanto, es necesario blindar los repositorios que albergan esas copias.

2. Tecnología **SIEM**[11]. La diversidad y especialización de las amenazas de seguridad actuales, junto con la complejidad y la envergadura de un entorno IT como BATERA, hacen prácticamente imprescindible disponer de herramientas que permitan centralizar la trazabilidad (*«logs»*) de los diferentes elementos de seguridad y automatizar el análisis de los mismos de cara a la detección de incidentes de seguridad y a la investigación de los mismos. Para que las herramientas de SIEM sean efectivas hay que incorporar todas las fuentes de eventos relevantes desde el punto de vista de la seguridad y, posteriormente, crear reglas de correlación que permitan analizar automáticamente los eventos en busca de actividades sospechosas o incidentes de seguridad. La calidad de las diferentes soluciones reside, sobre todo, en la calidad de las reglas de correlación que proporcionan, dependiendo esa calidad de la efectividad, actualización, respuesta a incidentes recientes y globales; en definitiva, de la fiabilidad de los eventos que ofrece el SIEM después de su análisis.

3. Soluciones **EDR**[12]: el puesto de trabajo, el dispositivo móvil o los servidores (*«endpoints»*) constituyen la puerta de entrada principal a través de la cual los/as atacantes comprometen a las organizaciones. Para poder hacer frente a estas nuevas amenazas se requieren productos que sean capaces, por una parte, de detectar automáticamente patrones de comportamiento anómalos que resulten sospechosos de constituir una amenaza y, por otra, de reaccionar a esa detección deteniendo la amenaza.

«“Zero Trust”: nunca confíes, siempre verifica»

4. **Gestión de Identidades**. En el mundo actual la información está en todas partes (la nube) y se consume desde cualquier dispositivo. Es debido a este cambio de paradigma que la **identidad** pasa a convertirse en un pilar básico y fundamental de la estrategia de Ciberseguridad de las organizaciones. A partir de esta idea surgen iniciativas como *«Zero Trust»* (confianza cero) que consiste en: *«nunca confíes, siempre verifica»*. La tendencia de mercado apunta a la identidad como un aspecto prioritario en los siguientes ámbitos:

- Aplicaciones y recursos en Cloud
- Cumplimiento normativo (RGPD)
- Colaboración sin límites
- Nuevas formas de autenticación *«passwordless»* (sin contraseñas) con mayores niveles de seguridad
- Tendencia a «Zero Trust»

Como vemos, a medida que las amenazas de ciberseguridad avanzan, el mundo de la seguridad informática también evoluciona. ❑

[11] **SIEM:** Tecnología que permite identificar y contener amenazas. Es capaz de recoger información de múltiples fuentes y, mediante mecanismos de agregación e inteligencia contextual, ofrecer altas capacidades para la monitorización y respuesta. Facilita y acelera los tiempos de detección y protección.

[12] **EDR:** son las siglas de «Protección de los sistemas expuestos»

ALBOAN:

Consejos sobre Windows10 y Office365: «Teams», una nueva forma de trabajar en equipo

«La funcionalidad más importante que ofrece Teams es la videollamada»

Son muchos los productos que nos ofrece Microsoft dentro de su paquete Office365. Hoy nos centraremos en una herramienta que muchas personas han descubierto durante la cuarentena que nos ha tocado vivir a raíz de la crisis sanitaria provocada por el coronavirus Covid-19, nos estamos refiriendo a *«Teams»*.

FUNCIONALIDADES

«Los "Equipos" pueden ser privados o públicos (abiertos)»

Teams (palabra inglesa que en castellano significa *«Equipos»*) es, básicamente, una plataforma unificada de comunicación que combina un chat, opción de hacer videollamadas y una zona para almacenar e intercambiar documentos, todo ello para facilitar la colaboración entre las personas que conforman un equipo de trabajo. Teams (que sustituye a Skype Empresarial) es, en definitiva, la aplicación que nos permite trabajar en grupo aunque físicamente estemos separados.

Dentro de Teams se manejan dos conceptos:

1. **Equipos**: son los grupos de personas, contenidos y herramientas relacionados con algún proyecto de la empresa. A la hora de crear un nuevo «equipo» debemos ser conscientes de que estos pueden ser **privados** (sólo las personas invitadas tienen acceso a él) o **públicos y abiertos** (donde todos los integrantes de la empresa pueden unirse). Por lo tanto, los miembros del equipo serán los únicos que podrán ver las conversaciones, los archivos y las notas publicadas en los canales.
2. **Canales**: son los apartados que se crean dentro de un Equipo para mantener las conversaciones organizadas o clasificadas por temas o por proyectos específicos. Los archivos que se comparten dentro de un canal (y que quedan recogidos en la pestaña «Archivos») en realidad se están almacenando en un SharePoint que se crea automáticamente. Los canales, en resumen, son el lugar donde se desarrolla la conversación del equipo y en los que se lleva a cabo el trabajo colaborativo.

VIDEOLLAMADAS

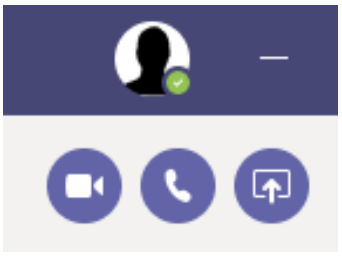
Teams ofrece actualmente distintas utilidades, como son:

- ✓ Compartir ficheros
- ✓ Realizar videollamadas
- ✓ Un «wiki»
- ✓ Un Calendario
- ✓ Un Chat

Para muchas personas la funcionalidad más importante que ofrece Teams (y que más se ha usado durante el confinamiento) es, sin duda, la **videollamada**.

Para iniciar una videollamada con otra persona es suficiente con entrar en Teams (vía web o a través de la aplicación que podemos instalar en nuestro ordenador) y buscar el nombre de esa persona en el directorio de la empresa y, a continuación, pulsar el botón de la llamada.

En cuanto la otra persona reciba en su ordenador el aviso de nuestra llamada y pulse el botón de «responder», podremos comenzar la conversación.



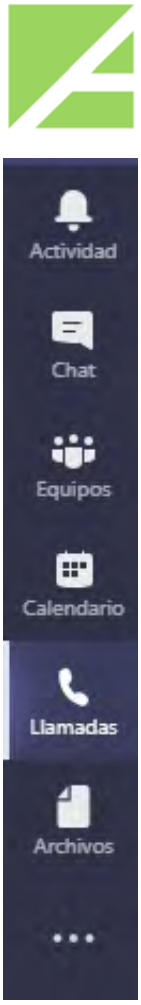
Con la idea de no perder el tiempo localizando a una persona que en ese momento no puede atendernos, bien porque está ausente o bien porque está ocupado con otra conversación, Teams, aparte de estar conectado con el Calendario de Outlook donde podemos ver si esa persona está en una reunión, nos permite saber, mediante una marca que aparece junto a su foto si está libre u ocupada. Si la marca es verde, eso significa que la persona se encuentra en su puesto de trabajo y está libre (es decir, disponible) para atender nuestra llamada, mientras que si la marca es roja, significa que no nos podrá atender ya que está ocupada.

El servicio de videollamada no está limitado a una conversación entre dos personas, sino que permite crear videollamadas/conversaciones en las que intervengan varias personas simultáneamente sin ningún problema.

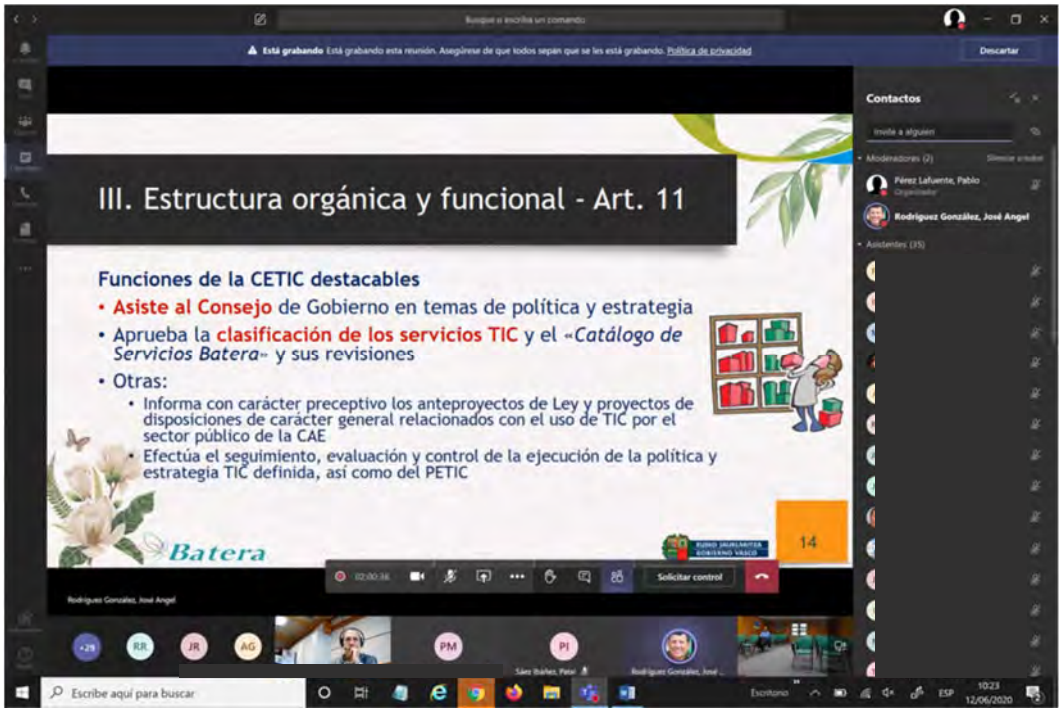
Otra opción muy interesante que ofrecen las videollamadas es la de **compartir documentos**. Esta opción nos deja compartir con el resto de compañeros/as que participan en una conversación un documento que tengamos en nuestro ordenador y que queramos mostrar durante la reunión para explicar algún tema concreto.

Para poder usar Teams es suficiente con que ya nos hayan migrado el ordenador al nuevo Office365 y que nuestro ordenador disponga de una webcam, unos altavoces y un micrófono (o unos cascos). Dado que el servicio de llamadas es **multiplataforma**, también se puede atender las videollamadas directamente desde el **teléfono móvil** (para ello, lo único que tenemos que hacer es instalar la *app* correspondiente).

No olvidéis que una imagen vale más que mil palabras, así que animaos y empezar a usar Teams. ❑



Web de acceso al portal del nuevo Office365:
https://portal.office.com



Contraportada

Nº 72
junio 2020

AL CIERRE

«Ni.eus», el servicio de email en euskera

La Fundación PuntuEUS y la empresa vasca Guebs han desarrollado recientemente un servicio de **correo electrónico** en euskera denominado «ni.eus».

El correo electrónico ni.eus permite el uso del dominio .EUS en las relaciones digitales interpersonales: en versión gratuita en el dominio ni.eus (por ejemplo: ximun@ni.eus) o en el caso del plan *«premium»*, personalizando el dominio .EUS (por ejemplo: info@ane.eus o kaixo@mendielkartea.eus).

Foto: web de Domeinuak.eus

Este nuevo servicio está dirigido a personas «euskaldunes» que hagan uso de Internet, particulares, asociaciones y empresas.

Uno de los aspectos más relevantes de este nuevo servicio de correo es la **privacidad**. Ni.eus garantiza la privacidad y seguridad de los datos de las personas usuarias: sin anuncios, sin *«tracking»* y comunicaciones cifradas. En definitiva, no incluye ningún anuncio ni realiza ningún seguimiento del uso por parte de las personas usuarias.

Además, está disponible en cualquier lugar, ya que se puede configurar en el teléfono móvil o en el ordenador, y también se puede utilizar online a través del *webmail*. Además, ofrece servicios adicionales como calendario, libreta de direcciones, redirecciones, etc.

Más información en:
https://www.domeinuak.eus

PROTAGONISTAS

June Almeida, la científica que descubrió los coronavirus

June Dalziel Almeida (nacida en Glasgow el 5 de octubre de 1930 y fallecida en Bexhill el 1 de diciembre de 2007) fue una viróloga escocesa que, con poca formación reglada, se convirtió en Doctora en Ciencia y pionera en la identificación, diagnosis y obtención de imágenes de distintos virus. De hecho, fue la primera persona en ver un coronavirus en un microscopio usando técnicas que ella misma desarrolló.

Foto: web de National Geographic

A los 16 años tuvo que dejar los estudios porque no tenía los recursos económicos suficientes para asistir a la universidad, y entró a trabajar como técnica en histopatología en la Glasgow Royal Infirmary. Poco después se trasladó al Hospital St. Bartholomew (Londres) para continuar con su carrera. El 11 de diciembre de 1954 se casó y se trasladó a Canadá, donde trabajó en el Ontario Cancer Institute como electromicroscopista. A pesar de tener poca formación reglada, fue promocionando debido sobre todo a las capacidades que mostraba.

Posteriormente, en 1964, A. P. Waterson, Profesor de microbiología en la escuela St. Thomas's Hospital Medical School, la convenció para que regresase a Inglaterra y trabajase en su hospital. Allí fue donde desarrolló un método para mejorar la visualización de los **virus**. Trabajó principalmente con el virus de la hepatitis B y los virus del resfriado común. Gracias a ese trabajo, June Almeida produjo las primeras imágenes del virus de la rubeola usando un microscopio electrónico. Poco después, en 1967, cuando June Almeida tenía 34 años, junto al Profesor David Tyrrell, trabajó en la caracterización de un nuevo tipo de coronavirus. Esta familia incluye el virus SARS y el SARS-CoV2, virus que causa el hoy en día famoso **Covid-19**.

Más información en:
https://es.wikipedia.org/wiki/June_Almeida