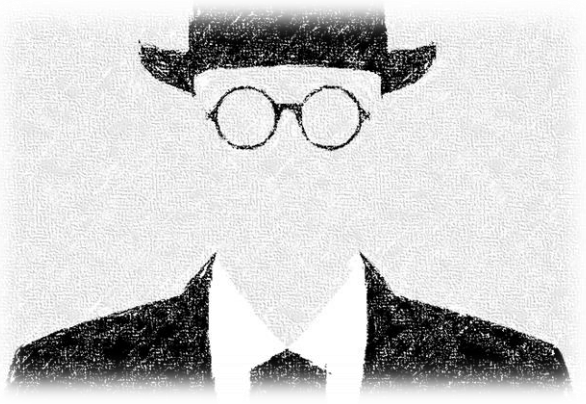

SUPLANTACIÓN DE IDENTIDAD

autelsi
Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información

Grupo de Regulación de AUTELSI

Julio 2021

INTRODUCCIÓN

La suplantación de identidad se entiende como aquella actividad por la que una persona se hace pasar por otra usando, habitualmente, medios informáticos. Este fenómeno se produce asiduamente en la actualidad, debido al aumento exponencial de la comunicación y uso de medios telemáticos. Asimismo, la mayoría de las actividades económicas llevadas a cabo por las empresas en el presente, requieren del uso de nuevas tecnologías de la información, las cuales se encuentran expuestas a multitud de ciberamenazas en el ámbito de la seguridad de la información, entre las que cabe destacar la suplantación de identidad.

El presente trabajo tiene por objeto el análisis de las razones por las cuales es necesario examinar y reflexionar acerca del fenómeno de la suplantación de identidad, en la medida en que su materialización genera una serie de consecuencias y efectos a nivel estructural, tanto a la propia empresa afectada, como en los clientes y consumidores de ésta.

Debido a su naturaleza, así como a su repercusión y alcance, se estima necesario analizar el fenómeno de la suplantación de identidad, sus tipologías, consecuencias legales derivadas y medidas a aplicar en caso de su materialización.

En este sentido, el trabajo llevado a cabo se estructura en un análisis desde dos puntos de vista diferenciados. En primer lugar, se examina la suplantación de identidad en el ámbito de la propia empresa, estudiando qué grado de responsabilidad se le debe exigir y qué medidas puede adoptar ésta para reaccionar y minimizar riesgos. En segundo lugar, se observa la suplantación de identidad y su afectación en los clientes, consumidores y empresas finales, examinando el grado de responsabilidad exigible a la empresa y las medidas a adoptar para reaccionar y minimizar riesgos.

SUPLANTACIÓN DE IDENTIDAD A LA EMPRESA

En el presente apartado vamos a analizar la suplantación de identidad que puede sufrir **una empresa o el empleado de una empresa**, analizando, en primer lugar, qué métodos son los más habituales de los utilizados en la práctica. Posteriormente, se analizarán las buenas prácticas objeto de recomendación, y concluiremos con el análisis de la responsabilidad que es exigible a la entidad suplantada.

(Pulsando aquí puede acceder a la hoja Excel de Suplantación de Identidad a la Empresa)

1.- Métodos más habituales utilizados en suplantación en la actualidad.

El fraude online se ha convertido en una de las principales preocupaciones de las empresas españolas. En 2020 supuso unas pérdidas anuales de más de 1 millón de euros de media para cada una de ellas, según el *"Informe sobre el estado del fraude en España 2019-2020",* elaborado por la Asociación de Empresas Españolas Contra el Fraude.

Debido a la facilidad con la que se puede crear un perfil en una red social (simplemente con un correo electrónico), **los casos de suplantación de identidad se han multiplicado**.

Se considera que se ha cometido suplantación de identidad de una persona física o jurídica cuando un atacante obtiene información personal y la utiliza ilegalmente para obtener algún beneficio. Está tipificado como delito en el Código Penal.
Esta información de la persona que conforma su identidad no tiene por qué ser necesariamente sus claves bancarias, registros médicos u otra información profundamente privada y de difícil acceso. Sólo el nombre, teléfono, domicilio o fotografías ya constituyen información identitaria y por tanto puede ser susceptible de ser suplantada.

Generalmente, lo que motiva a la suplantación de identidad suele ser:

1. **La realización de actividades fraudulentas de tipo económico** como la sustracción del saldo de cuentas bancarias, compras online o domiciliaciones indeseadas.
2. **Suplantación de la identidad de la víctima**: ya sea creando cuentas nuevas o modificando las ya existentes para que el afectado no pueda acceder a ella
3. **Publicación en nombre del afectado contenidos que le sean perjudiciales** (normalmente movidos por el chantaje y la recompensa económica)
4. **Comisión de un delito bajo una identidad falsa**
5. **Obtención de préstamos bancarios**

Fraude del CEO

Una forma común de suplantación de identidad que afecta a empresas es el denominado **Fraude del CEO**. Este tipo de ciberataque puede afectar a cualquier tipo de empresa y es cuando se produce una **suplantación de la identidad del CEO** para apropiarse de forma indebida de activos de valor.

Los ciberdelincuentes suplantan un alto cargo de la compañía con el propósito de engañar a los empleados para que, en la mayoría de los casos, efectúen órdenes de pago fraudulentas.
Estudian a las víctimas y recaban información sobre la empresa. Una vez conocen el organigrama y las operaciones habituales de la compañía, suplantan la identidad del CEO o de un alto cargo de la organización. Puede hackear su cuenta correo o de la creación de una dirección falsa. Luego, inician el envío de correos electrónicos o rondas de llamadas para solicitar el pago a un tercero, siempre de forma urgente y confidencial.

Phising

El **Phishing** es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.

Otros: Fraude de facturas

En este caso, los ciberdelincuentes estudian las empresas a través de su página corporativa, redes sociales e incluso hackeando las cuentas de correo de los empleados. Su objetivo es descubrir las relaciones que mantienen con sus proveedores.
El ciberdelincuente suplantará al proveedor y se pondrá en contacto con la empresa para solicitarle un nuevo procedimiento de pago facilitando un nuevo número de cuenta bancaria fraudulenta.

Otros: Pharming

El pharming envía a los usuarios a un sitio web fraudulento cuyo aspecto es el mismo que el del sitio web legítimo en el confían. No es necesario que las víctimas hagan clic en un enlace malicioso para llevarles al sitio falso. Los atacantes pueden infectar el ordenador del usuario o el servidor DNS del sitio web y redirigir al usuario a un sitio falso, incluso si la URL correcta está escrita.

Cuando están en la web maliciosa, si intentan iniciar sesión o realizar otras operaciones, estarán proporcionando información al ciberdelincuente.

Cualquier empresa puede de ser víctima de estos fraudes. Por este motivo, la formación y la concienciación en ciberseguridad es determinante para que los usuarios sean capaces de reconocer el fraude y denunciarlo a tiempo.

2.- Buenas prácticas.

La principal diferencia en la suplantación de identidades corporativas frente a la suplantación de identidades externas reside en que la creación de identidades corporativas es responsabilidad de la propia organización: es quien dispone de los medios para crear estas identidades, y puede asegurar tanto su suficiencia como su seguridad, y aplicar medidas de seguridad adicionales en caso de que las actuales se revelasen como insuficientes.

Por lo tanto, la **Buena Práctica fundamental** que debe ser implantada es **dotarse de un Servicio de Identidad Digital Corporativa**, con capacidad de crear Identidades Digitales y de ofrecer interfaces para que otros sistemas y/o personas y/o entidades puedan verificar que las identidades digitales con las que interactúan corresponden genuinamente con quienes dicen ser.

Este Servicio de Identidad Digital Corporativa puede apoyarse en diversas herramientas (Directorios, Metadirectorios, Bases de Datos, …), modelos de servicio (Metadirectorio, centralizados, federados, …) e incluso pueden basarse en recursos propios de la compañía, externos a la misma o en modelos mixtos. Cada organización deberá identificar y aplicar la solución más adecuada a sus necesidades y casos de uso.

Una vez establecida esta medida básica de protección, existen medidas adicionales que pueden ser de utilidad para enfrentar las amenazas identificadas previamente. Comencemos por las **medidas técnicas**

T1. **Autenticación de usuario en acceso a servicios empresariales**: La exigencia por la compañía de que el acceso a sus servicios sea autenticado permite que sean de aplicación las medidas de aseguramiento de la identidad y de protección de la misma que surgen de un Servicio de Identidad Digital Corporativo. Los servicios accesibles sin autenticación deberían ser los mínimos posibles, e idealmente, todos ellos estarían autenticados.

T2. **MFA**, o factor de autenticación múltiple: Cuando realizan un ataque, los atacantes tienen una esperable tendencia a utilizar usuarios con credenciales de autenticación que ya conocen, o que sean sencillas, predecibles, interceptables y/o con problemas de diseño. El uso de un doble factor de autenticación reduce en órdenes de magnitud la viabilidad de este tipo de ataques, en tanto que el acceso a uno de los métodos de autenticación es insuficiente para completar el ataque.

T3. **OSINT** y vigilancia digital: La detección y eliminación de servicios externos al control de la compañía y que pudieran ser confundidos con servicios de la compañía es una base de trabajo sólida para evitar ataques de pharming y otros que suplanten la identidad de la corporación ante clientes y otras entidades

T4. Utilización de mecanismos de **reputación y confianza** en el intercambio de mensajería. El uso de técnicas como SPF o DKIM permiten asignar un grado de confianza en la fuente de quien se reciben correos electrónicos y, en combinación con otras medidas clásicas

(antispam, filtros de contenido, antivirus de pasarela, etc), permiten descartar posibles vectores de ataque antes de que estos lleguen al usuario final y puedan convertirse

T5. El control de la **superficie de exposición** en correo electrónico y servicios de mensajería mediante la la apertura controlada de interconexiones (relays, canales de mensajería) para el intercambio de información con otras entidades. En particular, permiten concentrar la aplicación de las medidas de seguridad señaladas en el punto anterior en un número limitado de interconexiones y por lo tanto reduciendo el esfuerzo necesario en despliegue, seguimiento y monitorización de estas medidas de seguridad.

T6. Los dos puntos anteriores (mecanismos de reputación y reducir la superficie de exposición) deben ser contemplados, no solo para el **tráfico** entrante a la organización, sino también para el **saliente**. De esta forma, la organización puede asegurar que todas las comunicaciones que emite son legítimas y ofrece a sus interlocutores un criterio fiable para discriminar las comunicaciones efectivamente enviadas desde la misma, de las comunicaciones que solo aparentan este envío y que, por lo tanto, pueden ser descartadas por sus receptores, lo que reduce los riesgos de suplantación de identidad corporativa ante otras organizaciones.

T7. Y, por supuesto, el **desarrollo seguro** de servicios web, incluyendo el control de contenidos de terceros soportados en los servicios, chequeos de integridad, gestión de vulnerabilidades, parches y versiones, y la realización de pruebas de penetración periódicas.

Respecto de las medidas legales que podrían ser de aplicación en este escenario

L1. Contratación de **ciberseguros**, que doten a la organización de una compensación ante este tipo de incidentes, de ocurrir.

L2. Inclusión de **cláusulas** contractuales en los contratos con **empleados** relativas a sus funciones en seguridad de la organización, el compromiso de la persona de cumplimiento de estas funciones, el compromiso de la empresa para capacitar a la persona y las consecuencias de un posible incumplimiento.

L3. Inclusión de **cláusulas** contractuales con **proveedores, suministradores, clientes** y otras terceras partes relativas al compromiso entre las partes de colaboración en seguridad, las responsabilidades adquiridas en esta colaboración para colaborar en la protección propia y del resto de participantes, y las consecuencias de un posible incumplimiento.

L4. El **Registro de las actividades** que se realizan sobre los sistemas y la adecuada custodia de estos registros para su posible utilización en procesos penales posteriores que pudieran iniciarse como consecuencia de incumplimientos contractuales, brechas de seguridad y/o privacidad, y también para evidenciar el cumplimiento regulatorio en esta materia que le sea aplicable a cada organización.

Por último, y respecto de las medidas organizativas que pueden aplicarse para la prevención y respuesta ante estas amenazas

O1. Probablemente, la segunda medida más eficaz de todas las propuestas sea la correcta **formación y concienciación de las personas**. Los ataques de suplantación de identidad se basan en muchos casos en técnicas de ingeniería social, de engaño e inducción al error en las personal y/o en fallos humanos de operación de los sistemas, acceso a los mismos o custodia de contraseñas. La implantación de un programa de formación y concienciación sólido y completo que capacite al personal para identificar los intentos de ataque que vayan dirigidos hacia su persona o que la utilicen como eslabón débil de la cadena, va a redundar en que muchos si no todos los ataques que se le dirijan y que hayan superado las demás medidas de seguridad, van a tener una última medida de seguridad adicional en las conductas de las personas.

    En este punto, debemos tener en cuenta que la cultura media en ciberseguridad existente en la sociedad aun no es suficientemente alta, y que los problemas de suplantación de identidad ocurren tanto en el ámbito empresarial que se aborda en este documento, como en la esfera privada. Y que la formación en ciberseguridad le debe ser útil a la persona en ambas esferas para que la persona la aplique correcta y efectivamente.

O2. Monitorización y aprobación con confirmación de **cambios en las entidades** con las que nos relacionamos. Procesos tales como el cambio de apoderados, de puntos de contacto, de condiciones de pago o cobro, o el propio de abono de las facturas deberían tener incorporado que su ejecución requiera una doble validación del cambio por dos personas o procesos independientes, antes de su efectiva ejecución. Esta medida es un caso claro en el que la segregación de funciones aporta una mayor garantía y fiabilidad en las tareas ejecutadas y previene errores e incidentes posteriores.

O3. **Verificación previa y adicional de actividades inesperadas**. Como parte del programa de formación de personas y de los procesos de la organización, se debe incluir que, ante peticiones inesperadas realizadas por canales no habituales, debe realizarse una segunda comprobación de la veracidad de la misma. Esta petición debe realizarse de forma directa al originador de la petición y por un canal habitual y distinto del usado en la petición original.

3. Responsabilidad de la entidad

A la hora de producirse una suplantación de identidad en el ámbito de la empresa o que afecte a un determinado empleado de una organización, debemos atender a distintas dudas que se suscitan en la práctica:

- **¿Qué responsabilidad civil frente a terceros puede tener una empresa que es suplantada?**

El Código Civil determina que cualquier persona que cause un daño por acción u omisión mediante culpa o negligencia está obligado a reparar dicho daño causado (art. 1902 y ss CC). De esta forma, cuando se produce una suplantación de la identidad de un empleado de la empresa o de la propia empresa, tal como el fraude del CEO, es posible que se genere un daño a terceros que generaría a priori un derecho del perjudicado a resarcir esos daños sufridos. La responsabilidad civil determinaría la obligación de la empresa de reparar el daño por los actos llevados a cabo por sus empleados, aunque este daño no haya sido producido directamente por ella. Además, debemos tener en cuenta que podría ser exigible un especial cuidado derivado de la "culpa in eligendo" y "culpa in vigilando"; la primera se definiría como aquella responsabilidad civil exigible a la empresa por los actos del empleado a quien eligió; la segunda hace referencia a la responsabilidad de la empresa por los daños causados por sus miembros o empleados de los que tiene un especial deber de diligencia o cuidado en sus actuaciones. No obstante, esta responsabilidad no se produce automáticamente, sino que, es necesaria llevar a cabo la prueba de relación o nexo causal entre la acción y el daño producido a un tercero. Además, en el caso de suplantación de identidad, la actuación perjudicial no se lleva a cabo por el trabajador de forma personal sino por un tercero que se hace pasar por este.

Para que exista responsabilidad deben de darse una serie de requisitos: i) Existencia de una acción u omisión generadora de una conducta imprudente o negligente atribuible a la persona o entidad contra la que la acción se dirige; ii) Existencia de una daño o lesión; y iii) relación causal entre el daño y la falta. De entre los criterios, debemos señalar que el más complejo de aplicar en los casos de suplantación de identidad de carácter empresarial es el relacionado con la relación causal entre daño y la conducta. En los hechos de suplantación de identidad, en la medida en que la acción dañosa proviene de un tercero, la relación de causalidad podría quebrar, no siendo exigible a la entidad suplantada ninguna responsabilidad por la suplantación sufrida.

No obstante, se podría ocasionar una culpabilidad derivada por la acción u omisión del empleado, cuando no se produzca toda la debida diligencia necesaria por parte de la empresa para evitar tal incidente. Esta posible responsabilidad cesará cuando se pruebe que se ha llevado a cabo el necesario grado de atención y diligencia para evitar la causación de cualquier tipo de daño o perjuicio. Deberá examinarse los medios y garantías implantados en función del riesgo al que esté expuesto. Es por ello que, para poder reducir la responsabilidad a la que se podría enfrentar la empresa, se ha de garantizar y demostrar que se ha adoptado la diligencia adecuada para prevenir el daño.

- **¿Podría sancionarse a la empresa por no establecer controles específicos para evitar la suplantación de identidad de la empresa?**

La responsabilidad que puede originarse para la persona jurídica desde el plano administrativo puede derivarse de lo estipulado en la legislación vigente en materia de protección de datos: Reglamento UE 679/2016 General de Protección de Datos (en adelante RGPD) y la Ley Orgánica 3/2018 de Protección de Datos personales y garantía de derechos digitales (LOPDGDD). De este modo, el RGPD obliga a que cualquier responsable de tratamiento aplique las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a la probabilidad y gravedad de que se materialice un riesgo para los derechos y libertades de las personas físicas. De lo contrario, la entidad podría ser sancionada por la Autoridad de Control en protección de datos competente.
Emerge así el concepto de "Diligencia Debida", mediante el que se determina la obligada evaluación de los riesgos que presente el tratamiento de datos si se produjese destrucción, pérdida o alteración accidental o ilícita de datos, así como, una comunicación o acceso no autorizado. En esta línea, se establece como fundamental el análisis de riesgos del tratamiento de datos atendiendo a las circunstancias concretas de la empresa, tales como volumen y tipología de datos. Es de vital importancia establecer e implantar en una empresa los procedimientos y medidas necesarios, en función de las características y entidad de la misma, que permitan demostrar que se ha tenido una debida diligencia a la hora de intentar evitar que se produjese una suplantación de identidad en su seno. Así, aunque el perjuicio haya sido realizado por un tercero ajeno a la empresa, se ha de poder demostrar que se han adoptado las necesarias precauciones durante el desarrollo de la actividad empresarial, establecidas por la ley o el buen sentido, para evitar un daño que fuera previsible. Se trata de tener un nivel de cuidado objetivo atendiendo a las concretas circunstancias del caso que posibilite hacer patente que se estaba al tanto de la posibilidad de sufrir una suplantación de identidad, y que, con ello, se aplicaron las medidas oportunas para reducir la concreción de tal riesgo al mínimo posible.

- **¿Cómo debe gestionarse el incidente de seguridad?**

El Reglamento General de Protección de Datos obliga a comunicar a la Agencia Española de Protección de Datos sin dilación indebida, las brechas de seguridad salvo que se sea improbable que la violación pueda constituir un riesgo para los derechos y libertades de las personas físicas. De este modo, debe examinarse si la brecha sufrida, generalmente de confidencialidad, supone un riesgo para los derechos y libertades de los interesados; y en caso de respuesta afirmativa, debe notificarse. En los casos que exista un alto riesgo para los derechos y libertades de las personas físicas, debe notificarse al interesado. Además de las notificaciones, debe documentarse la brecha sufrida, con inclusión de los hechos, los efectos y las medidas correctivas adoptadas. Actualmente, encontramos ante la Agencia Española de Protección de Datos diversas actuaciones de inspección que han acabado en archivo de empresas que han resultado suplantadas en su integridad y que han procedido a realizar la notificación obligada (Procedimiento E/07708/2020).

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS, en lo que respecta a las obligaciones de comunicación de incidentes se transpone por el Real Decreto 43/2021, de 26 de enero. Esta normativa obliga a gestionar y resolver los incidentes que sufran los operadores de servicios esenciales y los proveedores de servicios digitales, pudiendo recabar la colaboración del Equipo de Respuesta ante Incidentes de Seguridad Informáticas (CSIRT por sus siglas en inglés).

El Real Decreto establece que la suplantación , entendida como el tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos, se califica con un nivel de peligrosidad medio. Las entidades sujetas a la normativa NIS estarán obligadas a notificar a las autoridades competentes aquellos incidentes relacionados con suplantación de identidad que tengan efectos perturbadores significativos.

- **¿Qué puede hacer la empresa si se suplanta la identidad de una empresa porque un empleado infrinja las normas de seguridad que previamente se han establecido? ¿Puede la empresa repetir frente al trabajador incumplidor?**

En cuanto a la responsabilidad personal del empleado frente a su empresa, hay que acudir a la legislación específica laboral para su esclarecimiento. El Estatuto de los Trabajadores determina que los trabajadores tienen como deber básico "*cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia".*
La entidad ante la transgresión de la buena fe contractual y su diligencia exigible podrá sancionar al empleado. En los casos más graves, podrá llegar incluso al despido del empleado. Sobre la procedencia del despido, resulta esclarecedora la reciente **Sentencia de la Sala de lo Social del TSJ de la Comunidad Valenciana de 22 de junio de 2021** por la que se declara procedente el despido disciplinario de una directiva, tras sufrir una estafa informática por un importe superior a los 4 millones de euros. Concretamente, la Sala determina que existe una "*grave transgresión de la buena fe contractual*" que ha dado lugar a un perjuicio económico sustancial para la empresa en la medida en que la actora no atendió a una "*elemental prudencia*". La sanción del despido es proporcionada a la gravedad de los incumplimientos que se han producido, dado que, existe una "*falta absoluta de criterio*" y una "*grave negligencia*" en la actuación de la empleada, derivada de otorgar a los presuntos estafadores documentos firmados por sus superiores sin unas mínimas comprobaciones previas.

Además, la empresa tiene podría repetir frente al empleado por el daño causado. Para ello, se ha de iniciar un procedimiento declarativo de responsabilidad civil frente al empleado probando los daños y perjuicios que haya tenido que asumir la empresa, la negligencia que se ha producido y el nexo causan entre el daño y la culpa atribuible al empleado.

- **¿Qué medidas legales puede adoptar la empresa frente al ciberdelincuente que le ha suplantado?**

La empresa deberá denunciar los hechos ante las Fuerzas y Cuerpos de Seguridad del Estado, Ministerio Fiscal o los Juzgados de Instrucción competentes territorialmente para conocer de estas actuaciones delictivas. En el caso de que la entidad suplantada haya identificado al suplantador, podrá accionar por la comisión de los delitos que se hayan podido cometer (falsificación de documentos privados o públicos, estafas, delito de hacking, entre otros). Actuando la suplantada como perjudicada, podrá ejercitar ante la jurisdicción penal la acción civil y penal conjuntamente. También podrá reservarse la acción civil de resarcimiento de daños y perjuicios para ejercitarla ante los Juzgados de Primera Instancia una vez concluido el procedimiento penal.

SUPLANTACIÓN DE IDENTIDAD AL CLIENTE FINAL

En el presente apartado vamos a analizar la suplantación de identidad que puede sufrir **el cliente o usuario final** de cualquier entidad u organización. Se identifica, en primer lugar, las fases en las que se puede producir la suplantación de identidad. En segundo lugar, se analizan las amenazas aplicables para cada una de esas fases y, posteriormente, se proponen los controles o buenas prácticas que pueden ser adecuados para cada amenaza. Se concluye el examen con el análisis de las responsabilidades exigibles a la entidad suplantada.

(Pulsando aquí puede acceder a la hoja Excel: Suplantación de Identidad al Cliente Final)

1.- Fases en las que se puede producir la suplantación de identidad.

Las actividades habituales de cualquier entidad puede dar lugar a que se pueda generar una situación de suplantación de identidad. Resulta adecuado sistematizarlas por las distintas fases en las que puede suceder.

Primera fase: Registro de identidad / On boarding.

Es la fase inicial donde el usuario aporta sus Datos, por los diferentes canales posibles permitidos (puede ser in situ o en remoto) con el fin de ser registrado en el sistema o aplicación y conseguir le sea asignada su identidad y credenciales iniciales con las que poder acceder posteriormente.

Segunda fase: Identificación y autenticación. Uso de servicios y firma de operaciones

En esta segunda fase se encuentra el proceso necesario para lograr acceder mediante las credenciales de usuario asignadas donde se produce una validación y autenticación, normalmente robusta de dos o más factores (algo que se sabe, algo que se tiene, algo que se es, algo basado en el comportamiento) que da paso a los servicios y operativas a realizar conforme al perfil del usuario que se le asigno. En cuanto al uso de servicios y firma de operaciones, es un momento en el procesos claramente diferenciado y es uno de los momentos donde mayor riesgo puede existir, en el uso de las credenciales de firma, normalmente diferentes y complementarias a las de identificiación y autenticación y, además, apoyadas por sistemas de scoring de riesgo de operaciones e Inteligencia Artificial.

Tercera fase: baja y eliminación de la identidad digital

Se incluye en esta fase tanto la inactivación, bloqueo y baja y borrado del usuario y su identidad en el sistema o aplicación.

Fase transversal: Custodia, credenciales de identidad. Trazabilidad y registro de operaciones.

Además de las fases descritas, nos encontramos que las organizaciones desarrollan una actividad de carácter transversal consistente en la custodia de la identidad y sus credenciales y atributos tanto por la organización que la asigna, como por parte del propio usuario en todo

momento del proceso. y por otro lado también es transversal, toda la trazabilidad y registro en los sistemas de logging desde inicio a fin, para poder auditar y/o revisar en su caso en todo momento o ante incidentes o brechas de seguridad.

2.- Amenazas más comunes

En el presente apartado analizamos aquellas amenazas que son más comunes atendiendo a las fases. En cada caso indicamos el riesgo existente de que puedan llegar a materializarse. Las amenazas más comunes que identificamos en cada una de las fases son las siguientes:

Amenazas en la primera fase: Registro de identidad / On boarding.

- Phishing: ataque en los que los cibercriminales envían correos electrónicos fraudulentos que imitan el diseño de empresas conocidas. (Riesgo Alto)
- Smishing: ataque similar a phishing pero se utilizan mensajes de texto en forma de SMS o a través de las distintas aplicaciones de mensajería instantánea. (Riesgo Alto)
- Vishing: ataque similar al phishing pero se suplanta la identidad por vía de llamada telefónica. (Riesgo Medio)
- Spearphishing, Business Email Compromise o Fraude del CEO: Ataque consistente en robar fondos de las empresas suplantando la identidad de un alto directivo. Se suele realizar por email y reforzado con una llamada telefónica en la que la víctima se siente presionada. (Riesgo Alto)
- Email Spoofing: consiste en la falsificación del correo electrónico del remitente. (Riesgo Alto)
- Cibersquating: es el ataque en el que se suplanta el dominio web de una entidad reconocida cambiándole el nombre. (Riesgo Medio)
- Farming: radica en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad. (Riesgo Medio)
- Deepfakes: consiste en manipular archivos de video y audio que imitan las características biométricas de las personas como apariencia, expresiones faciales o la voz de una manera engañosamente real. (Riesgo Medio)

Amenazas en la segunda fase: Identificación y autenticación. Uso de servicios y firma de operaciones

- Ataques de suplantación de web o app de acceso simulando ser auténtica: consiste en simular una web o apps para capturar las credenciales de acceso y alimentar con ellas paneles de Command & Control o acceder para consultar información del usuario. (Riesgo Medio)

- Ataques de Man in the middle o man in the browser: consiste en impostarse en medio de la navegación del usuario para, usando el mismo sus propias credenciales, lograr desviar

información o fondos a otro lugar o cuenta. (Riesgo Alto)

- Ataques a las credenciales de autenticación por fuerza bruta: se utilizan ataques de diccionario, fuerza bruta de proceso, etc para logara claves de acceso. (Riesgo Medio)

- Ataques a credenciales de firma como desvíos de SMS con códigos OTP: Son aquellos que pueden ir dirigidos contra el propio dispositivo del usuario donde pueda recibir las credenciales de un solo uso (OTP por sus siglas en inglés) con el fin de capturarlas y operar luego con ellas, alimentando igualmente los paneles command & control o comerciando con ellas, como datos de tarjetas (Riesgo Alto)

- Ataques de ingeniería social: son ataques que utiizan técnicas de engaño y captura de datos y credenciales al usuario mediante llamadas falsas, encuestas, posibles premios, etc. (Riesgo Alto)

Amenazas en la tercera fase: baja y eliminación de la identidad digital.

- No existencia de políticas de bloqueo, inactivación y bajas de usuarios: de este modo, las credenciales pueden quedar expuestas mayor tiempo del debido, ser usadas sin control cuando ya no procede. (Riesgo Alto)

- Inexistencia de un proceso integral definido: supone que no exista un proceso integral que aplique las políticas de bloqueo, inactivación, baja y borrado de usuarios y credenciales en todos los lugares donde se hayan podido almacenar incluidos en copias de seguridad. (Riesgo Alto)

Amenazas en la fase transversal: custodia credenciales de identidad y trazabilidad y registro de operaciones.

- Fata de robustez en los sistemas de almacenamiento de credenciales y usuarios como bases de datos: esta cuestión otorga la posibilidad de atacar y extraer y exfiltrar de forma unitaria o masiva datos de usuarios y de sus credenciales de accesos. (Riesgo Alto)

- Inadecuado control y uso de credenciales por usuario: supone la falta de protección adecuada de estas, no segregar por usos diferentes con riesgo de que puedan ser capturadas y usadas o cesión de las mismas a terceros. (Riesgo Medio)

- No registrar todas las operaciones del usuario: implica que no se disponga de sistemas de logging activo con datos e información suficiente y que sean a su vez, sistemas seguros en si mismo, para poder trazar, monitorizar o luego revisar, auditar o hacer un análisis forense de los mismos ante incidencias o incidentes. (Riesgo Medio)

3.- Controles y buenas prácticas.

A continuación establecemos algunos controles y buenas prácticas que podrán ser tenidas en cuenta en función de la amenaza en concreto:

- Phishing: 1.- Acciones de concienciación; 2.- Acciones de ciberinteligencia para identificar malos usos de la información de la entidad.

- Smishing: 1- Instalación de antivirus, cortafuegos y otras herramientas de seguridad; 2 - Campañas de concienciación y sensibilización sobre ciberseguridad, para que el usuario/cliente adquiera buenas prácticas que le permita configurar y administrar su equipo de forma segura convirtiéndose en un "firewall humano".

- Vishing: 1- Instalación de antivirus, cortafuegos y otras herramientas de seguridad; 2 - Campañas de concienciación y sensibilización sobre ciberseguridad, para que el usuario/cliente adquiera buenas prácticas que le permita configurar y administrar su equipo de forma segura convirtiéndose en un "firewall humano".

- Deepfakes: 1.- Grabación y a prueba de manipulaciones almacenamiento del audio y sesión de video; 2.-participación activa del solicitante, incluido algún discurso; La falsificación de la voz de alguien es un proceso complejo, y si hay una grabación de audio Por lo general, es posible, mediante herramientas y practicantes forenses especializados, determinar si la voz es del solicitante cuya identidad digital está bajo escrutinio o no. La parte hablada podría no ser solo el nombre del sujeto o los datos generales (como el día y la hora), pero también un texto aleatorio, para proporcionar un segmento de audio más largo y una variación impredecible del proceso. 3.- Introduzca algunos elementos aleatorios en la prueba de identidad. Si el proceso sigue el mismo script, un atacante podría predefinir elementos específicos (como un video pregrabado) para reproducirlos más tarde según lo solicite el operador. Por el contrario, si hay algunos elementos aleatorios (como cambiar el orden de las preguntas o preguntar de la nada a levantar una mano, rotar la cara y gestos similares) esta línea de ataque falla. Además, cuando estos Los elementos aleatorios se relacionan con otras partes del cuerpo, hacen más costoso crear algún tipo de artefacto físico o digital que reemplaza al sujeto real, ya que podrían dejar más claro que el solicitante lleva una máscara facial, o que el artefacto digital que está frente a la cámara no ha sido modelado para incluir las otras partes del cuerpo. Este control también contrasta los ataques de repetición.

- Ataques de suplantación web o app o acceso simulado ser la auténtica: controles de crowling de stores, webs, dominios, monitorización avanzada y servicios especializados. junto con formación y cultura de ciberseguridad al usuario.

- Ataques man in the middle o man in the browser: construcción de aplicaciones y sistemas robustos, monitorizados y testados con técnicas de caja blanca, caja gris y caja negra que eviten vulnerabilidades en todo lo posible, además de pruebas de simulación de que el software hace solo lo que debe hacer.

- Ataques a credenciales de autentificación por fuerza bruta: exigir políticas de clave y

credenciales robustas y complejidad adecuada y autenticación, validación y firma de operaciones reforzadas con dos o más factores.

- Ataques a credenciales de firma como desvíos de SMS con códigos OTP: Protección Activa y Dinámica de Dispositivos, Aplicaciones y Sistemas y BBDD.

- Ataques de ingeniería social: Cultura y Formación en Ciberseguridad

- No existencia de políticas de bloqueo, inactivación o baja: generación de políticas de bloqueo. inactivación y borrado junto a formación y capacitación de usuarios sobre las best practises y también sistemas automáticos de revisión y bloqueo y auditorias activadas y periódicas.

- Inexistencia de un proceso integral definido: herramientas y opciones de auditoria activadas, revisiones periódicas de auditoria.

- Falta de robustez en los sistemas de almacenamiento de credenciales y usuarios: configuración y bastionado adecuado de los sistemas y bbdd, analisis periódico de vulnerabilidades conforme a guias y metodologias estandares como las ccn stic, owasp, etc.

- Inadecuado control y uso de credenciales por usuario: cultura de uso, sistemas de detección y validación.

- No registrar todas las operaciones del usuario: disponer de sistemas tipo siem para una gestión integral y integrada de logs, asi como herramientas tipo big data e ia que ayuden de forma temprana a detectar conductas anómolas o no usuales y a los procesos de auditoria y forrensics, conservando la cadena de custodia adecuadamente, incluso para prueba legal.

4. Sectores principalmente afectados.

Podemos indicar por fases los sectores principalmente afectados. De este modo podemos distinguir:

En la primera fase, referente al proceso de on boarding, los sectores que se encuentran mayoritariamente en una situación de mayor riesgo son el sector financiero y seguros, telecomunicaciones y retail.

Segunda fase relativa a la identificación, auntenticación y uso los principales sectores expuestos a las amenazas anteriores son: Banca, Telecomunicaciones, Retail, Salud, Jurídico, Legal e Industrial.

Tercera y cuarta fase relativas a la baja y eliminación de la identidad digital y a la custodia respectivamente, encontramos que no hay ningún sector especialmente expuesto, sino que a nivel general todos los sectores estarían expuestos.

5. Responsabilidad de la entidad

A la hora de producirse una suplantación de identidad de un cliente en el ámbito de la empresa existe el riesgo de causar daños al verdadero cliente suplantado, así como, a otros terceros interesados. Además, debemos de tener en cuenta distinta normativa específica que obliga a las entidades a establecer mecanismos de identificación de usuarios. De esta forma, se pueden originar ciertas responsabilidades para la organización derivadas de su carácter de persona jurídica. A continuación, se analizarán estas posibles responsabilidades desde los siguientes planos en formato preguntas y respuestas:

- **¿Están las empresas obligadas a identificar adecuadamente a sus clientes? ¿Qué normativa específica es de aplicación?**

Así es. La entidad está en la obligación de identificar a sus clientes de forma precisa. Para que sea válido un contrato debe concurrir, entre otros elementos, el consentimiento de los contratantes. Resulta necesario que se identifique a la persona que manifiesta la aceptación del contrato.

Existe normativa específica aplicable a determinadas empresas y organizaciones sobre requerimientos de identificación del usuario:

1) En primer lugar, la Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y financiación del terrorismo obliga a los sujetos obligados a identificar las personas físicas o jurídicas que *"pretendan establecer relaciones de negocio o intervenir en cualesquiera operaciones*" por medio de documentos fehacientes que permitan comprobar la identidad. El Reglamento de desarrollo de la Ley de Prevención de Blanqueo de Capitales, especifica que el principal método de identificación para operaciones que se realizan presencialmente será el Documento Nacional de Identidad en vigor, la Tarjeta de Residencia, el Pasaporte o la Tarjeta de Identidad de Extranjero. Mayor complejidad puede operarse en aquellas operaciones celebradas a distancia de forma no presencial, en las que la identidad debe poder acreditarse mediante **firma electrónica cualificada** o mediante la recepción de copia de los documentos necesarios de diligencia debida.

2) En segundo lugar, en el ámbito de las entidades bancarias. El Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en adelante, RDL 19/2018) que trae consecuencia de la Directiva (UE) 2015/2366 del Parlamento y del Consejo, de 25 de noviembre, sobre Servicios de Pago en el Mercado Interior, tiene por objeto el establecimiento de un marco normativo que aumente la seguridad de los usuarios en el uso de nuevos mecanismos tecnológicos de pago. El RDL 19/2018 establece que el proveedor de servicios de pago ha de adoptar obligatoriamente medidas de seguridad adecuadas y necesarias para asegurar tanto la identidad del ordenante como la autenticación de la operación. De hecho, solo se consideran autorizadas las operaciones de pago cuando el ordenante haya dado el consentimiento para su

ejecución y en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a este el importe de la operación no autorizada de inmediato. El ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado fraudulentamente, debiendo ser probada tal actuación por parte de la entidad bancaria. Los Tribunales nacionales han concretado en numerosas ocasiones que las entidades bancarias son responsables frente a sus clientes cuando estos sufran una suplantación de identidad o phishing.

3) El Reglamento UE 910/2014 de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/83/CE (Reglamento eIDAS) establece las normas aplicables para la identificación electrónica. A los sistemas de identificación electrónica les es exigible unos determinados niveles de seguridad en función del grado de confianza necesarios para establecer la identidad de la persona. Se establece también el régimen de responsabilidad aplicable a los prestadores de servicios de confianza de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica por el incumplimiento de las obligaciones que establece la normativa. Los prestadores de servicios de confianza deben adoptar medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan. La normativa europea se complementa con la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza que establece que la identidad del titular de un certificado cualificado de confianza exigiría que la persona física se personare ante el encargado de verificar la identidad debiendo aportar DNI, pasaporte u otros medios admitidos para identificarse; además, se consideraría equivalente los métodos de identificación reconocidos que aporten una *seguridad equivalente en términos de fiabilidad a la presencia física* y cuyo nivel de seguridad resultare certificado.

- **¿Qué responsabilidad civil puede exigirse a la empresa ante la suplantación de identidad de un cliente?**

En el caso de que un cliente reciba una suplantación de identidad en el marco de una empresa, esta podrá ser responsable de los daños y perjuicios que se le hayan generado si se llegase a acreditar que la entidad ha incurrido en negligencia, dolo o ha incumplido una relación contractual. El supuesto más común será la intervención de culpa o negligencia de la entidad. Para que la entidad tenga la obligación de reparar el daño causado por culpa o negligencia han de confluir diferentes elementos: (i) contrato entre las partes; (ii) incumplimiento de las obligaciones estipuladas; (iii) falta de diligencia o previsión; (iv) nexo o relación causal entre el hecho y el resultado; (v) generación de un daño o perjuicio reparable y cuantificable. En base a estas prerrogativas y dado que la acción dañosa proviene de un tercero, en principio no sería imputable la culpa contractual a la empresa.

La empresa ha de demostrar que aplicó todas las medidas pertinentes para evitar que se originar el daño. En este caso la suplantación de identidad debe implantar todas aquellas medidas necesarias en función del riesgo existente para prevenir tal acontecimiento.

- **¿Y si el perjudicado ha omitido unos mínimos exigibles de prudencia favoreciendo que se le suplante la identidad, debe responder en todo caso la empresa?**

En el caso de que el perjudicado pueda contribuir con su conducta imprudente a que se le suplante la identidad, la empresa podría exonerarse de responder frente al mismo. La protección de los consumidores se articula en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. Esta normativa declara como regla que, con carácter general, cualquier perjudicado que tenga la condición de consumidor sea indemnizado por los daños o perjuicios que se le causaren. Pero también se define que un prestador de servicios no será responsable de indemnizar aquellos daños y perjuicios que se hayan podido causar cuando se acredite que se ha cumplido con las exigencias y requisitos reglamentarios establecidos y los cuidados y diligencias que exige la naturaleza del servicio. Así, ante aquellos hechos de los usuarios que supongan un incumplimiento de las reglas mínimas de cuidado, la entidad quedaría exonerada. En aquellos casos en los que la negligencia del perjudicado no supone la desatención de las cuestiones más básicas esperadas, podría existir en su caso una concurrencia de culpas debiéndose moderar la responsabilidad exigible al prestador del servicio.

- **¿Opera igual la responsabilidad en el ámbito de servicios de pago?**

No, como hemos indicado anteriormente se sujetan a normativa específica que determina que el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado fraudulentamente, debiendo ser probada tal actuación por parte de la entidad bancaria. No obstante, el usuario únicamente obtendrá la rectificación por parte del proveedor de una operación de pago no autorizada o ejecutada incorrectamente se comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación. La entidad queda obligada a responder frente al cliente y a adoptar aquellas medidas de seguridad adecuadas para garantizar la identidad del ordenante de la operación. Así las cosas, opera una responsabilidad civil directamente exigible a los operadores de pago derivada del deber de vigilancia que han de prestar en cuanto al establecimiento de medidas de seguridad en las órdenes de pago emitidas por los clientes. Existe jurisprudencia que hace expresa referencia a la responsabilidad objetiva por un funcionamiento incorrecto en los servicios de banca electrónica – entre otras, Sentencia de la Audiencia Provincial de Alicante 107/2018 de 12 de marzo que menciona expresamente:

> *"Las medidas de seguridad no solamente están destinadas a proteger la seguridad de las órdenes de pago emitidas por los clientes sino que su eficacia exonera a las entidades de crédito de sus responsabilidades frente a las órdenes de pago no emitidas por sus clientes de tal forma que el incumplimiento de este específico deber de vigilancia da lugar a una responsabilidad por "culpa in vigilando" o responsabilidad objetiva por el mal funcionamiento de los servicios de banca electrónica"*

Así, existe responsabilidad bancaria por los defectos de seguridad del sistema que determina la ejecución de ordenes de pago no autorizadas por un cliente, excepto que el banco acredite culpa o negligencia del suplantado:

"Constituye por tanto obligación esencial de las entidades prestadoras del servicio de banca online el dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones por lo que, en el supuesto de insuficiencia o mal funcionamiento de las adoptadas, deben ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema."

- **¿Existiría incumplimiento de la normativa de protección de datos en los supuestos de suplantación de identidad? ¿Puede sancionarse a la empresa por infracción de la normativa de protección de datos?**

Sí, podría existir un incumplimiento de la normativa de protección de datos. Como hemos dicho, la entidad debe tratar datos exclusivamente cuando tenga legitimación para ello. En los casos de suplantación de identidad, la entidad está tratando datos personales sin base que legitime para ello, por lo que estaría incumpliendo el RGPD. Deben articularse medidas adecuadas para garantizar la identificación del usuario. La sanción aplicable estaría calificada como muy grave. La Agencia Española de Protección de Datos ya ha impuesto sanciones por esta cuestión, en tanto que no existe contrato alguno entre las partes que legitime el tratamiento de datos y, además, generalmente no se procede verificar la identidad de los interesados (PS/00308/2020 entre otras)

CONCLUSIONES

La suplantación de identidad está a la orden del día. Este hecho afecta a las entidades desde una doble perspectiva: la suplantación de identidad de los clientes o de los usuarios de cualquier organización; y la suplantación de la propia entidad o de alguno de sus empleados. Desde la doble orientación señalada, podemos destacar siguientes conclusiones:

- Resulta indispensable que se mejore la **concienciación y sensibilización** de los usuarios y de los profesionales que intervienen en los procesos de identificación. Es un factor nuclear y de vital importancia y que servirá a la entidad para acreditar diligencia debida.

- El **conjunto de los sistemas informáticos y tecnologías intervinientes deberán ser las adecuadas para evitar la suplantación de identidad y estar correctamente configurados**. Es responsabilidad de cada organización que el conjunto de sistemas estén debidamente bastionados.

- Debe mejorarse los **protocolos y procedimientos internos** que puedan ayudar a definir correctamente las funciones y responsabilidades de los intervinientes durante todas las fases donde se pueden producir una suplantación de identidad.

- Los procesos de identificación y autenticación de las organizaciones deben estar **alineados con el cumplimiento de la normativa vigente**. A estos efectos, las entidades tendrán que definir los mecanismos de identificación así como las técnicas empleadas conforme, fundamentalmente, al principio de proporcionalidad.

- Deberá favorecerse la **generación de la evidencia digital** que permita la trazabilidad en la investigación y generar prueba de carácter cualificada.

- Aquellos sectores que conservan mayor información del usuario, y especialmente los que tratan datos de mayor sensibilidad como son el sector financiero, asegurador, salud, retail o la Administración Pública, deberán prestar especial atención a las medidas para evitar la suplantación de identidad al usuario.

- Las novedades que incorpora el nuevo sistema de DNI otorga la posibilidad de reforzar los mecanismos de identificación y autenticación; la identidad digital soberana otorga al ciudadano el pleno control sobre su identidad digital. Además, actualmente, el Reglamento eiDAS está en fase de revisión, de tal forma que se actualizará el marco de identificación y autenticación de forma que se pueda obtener un mayor nivel de seguridad y de interoperabilidad.

En conclusión, desde el Grupo de Regulación de AUTELSI consideramos que la suplantación de identidad supone un riesgo que obliga a todas las organizaciones a aplicar la máxima diligencia posible. Constituye una obligación esencial que, tanto las entidades públicas como las privadas, tengan medidas técnicas que resulten especialmente apropiadas para la correcta identificación de sus clientes o usuarios, y en su caso mejoren y adecuen los protocolos y procedimientos a tal fin.