ANÁLISIS: INSIDERS

Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI)

Grupo de Trabajo de Calidad y Seguridad

Septiembre 2021

INDICE

1 Introducción sobre la problemática de los Insiders 7

2 Metodología de trabajo (reuniones comunes, trabajo por grupos de expertos…) 12

3 Identificación de los 13 perfiles de insider y su caracterización 13

4 Identificación de los 6 “momentos” a lo largo del ciclo de vida del insider. 17

5 Tipología de controles (administrativos, técnicos…) 18

6 En detalle, cuatro casos de uso paradigmáticos 19

7 Reflexiones finales 25

8 Fichas individuales para cada perfil (Tablas Excel) 27

Foto portada; fuente: https://www.pexels.com/photo/red-apple-fruit-with-hole-161615/

EXPERTOS DEL GRUPO DE CALIDAD Y SEGURIDAD DE AUTELSI QUE HAN PARTICIPADO EN LA ELABORACIÓN DE ESTE DOCUMENTO.

AGRADECIMIENTOS

En primer lugar, queremos manifestar nuestro agradecimiento a las empresas representadas en el Grupo de trabajo de Seguridad y Calidad de AUTELSI; y a sus vocales, que han contribuido activamente al desarrollo y resultado positivo de esta iniciativa. En especial queremos destacar la colaboración de los siguientes integrantes:

Lázaro Anguís, Francisco. **Presidente del grupo de Calidad y Seguridad de AUTELSI.** CISO y DPD de Renfe Operadora. Ingeniero de Telecomunicaciones. Profesor Asociado en la ETSI de telecomunicaciones de la Universidad Politécnica de Madrid. Con más de 25 años de experiencia en el ámbito de la seguridad de la información, posee la habilitación por el Ministerio del Interior como Director de Seguridad. Director del Centro de estudios de movilidad e Internet de las cosas (CEM) del ISMS Forum, Vicepresidente de la Asociación Española de Evidencias Electrónicas (AEDEL), Vocal en comisiones de normalización tales como el CTN 320 Ciberseguridad y privacidad o el Subcomité de Seguridad de las TI del CTN 196 Protección y Seguridad de los ciudadanos. Editor de la norma UNE 71505-1 Sistema de Gestión de Evidencias Electrónicas, y autor de diversos artículos y libros.

Álvarez, Luís Eladio, Ingeniero Superior Industrial del ICAI y Perito de la Corte de Arbitraje de la Cámara de Comercio de Madrid para el sector de las TICC. Lleva más de 30 años de experiencia profesional en el sector de las TIC desempeñando distintas responsabilidades, entre otras, en el área de Seguridad, llegando a ser Director de Tecnología, Operaciones y Seguridad de C.C. Carrefour durante 13 años. En la actualidad es especialista en estrategia de Seguridad.

Arbizu Luaces, Alberto, Responsable Grandes Cuentas Infoblox, Licenciado en Empresariales por la U.N.E.D, MBA por el Instituto de Empresa. Con más de 20 años de experiencia en Telecomunicaciones y Seguridad, ha trabajado como Country Manager en BlueCoat, Secure Computing o Efficient IP y en el desarrollo de negocio de Grandes Cuentas a nivel internacional en Enterasys y Juniper.

Alonso Ollacarizqueta, Icíar, Ingeniera Industrial. Jefa de Servicio de Nuevas Tecnologías y Sociedad de la Información del Gobierno de Aragón desde 2004. Ha participado en la elaboración del I y II Plan Director de la Sociedad de la Información en Aragón, así como en el proyecto de apertura de datos del Gobierno de Aragón y en la Estrategia Aragonesa de Open Data 2019/2022.

de la Huerga Ayuso, Mónica, CISO de Sopra Steria España. Cuenta con quince años de experiencia en la gestión y desarrollo de proyectos y servicios TIC en diferentes sectores de la industria en Europa. Los 4 últimos años, con dedicación plena a la seguridad de los sistemas de la información.

Díez Díaz, David, Ingeniero en Informática por la Universidad de León, con Certificado de Aptitud Pedagógica, período de docencia del doctorado Sistemas Inteligentes en la Ingeniería. Responsable de Seguridad y Sistemas en el Servicio de Seguridad de la Información, Junta de Castilla y León. Miembro del Grupo de Trabajo de Seguridad CCN de la Comisión Sectorial de Administración Electrónica.

García-Romanillos Henríquez de Luna, Javier, Information Security Officer en IAG GBS, sirviendo de enlace entre IAG y las operadoras Iberia, Iberia Express y Vueling. Con más de quince años de experiencia en el ámbito de la seguridad de la información, ha desarrollado gran parte de su carrera profesional como consultor y auditor de riesgos y tecnologías de la información en EY. Es Ingeniero Técnico Informático (UPSAM) y posee las certificaciones CISA, CISM y CRISC por ISACA; Lead Auditor ISO 27001 por BSI; Lead Auditor ISO 22301 por Tüv Nord; Experto Técnico por EuroPriSe; ITIL v3.

Gutiérrez González, José Antonio, Manager de Seguridad de la Información en GRUPO DIA. Con más de once años de experiencia en el ámbito de la ciberseguridad, ha desarrollado gran parte de su carrera profesional como Consultor de ciberseguridad en ATOS. Ingeniero Técnico Informático (UPSAM) con Master en Seguridad de la Información, posee las certificaciones CISA, ITIL v3, ISO 22301 y PCI-QSA (2012-2015).

Hernández González, Rafael, CISO de Cepsa, con más de 25 años dedicados a implementar y gestionar la seguridad de los servicios y sistemas. Ingeniero Superior de Telecomunicaciones. Director de Seguridad Física y Jefe de Seguridad (2016), homologado por el Ministerio del Interior. Miembro de la directiva del ISMS Fórum. Certificaciones en ITIL e ISO 27001. Responsable del SGSI Integrado de las Certificaciones ISO 20000 e ISO 27001. Colaborador en grupos y publicaciones.

Benito Gómez, Mariano J., Director de Seguridad / CISO de GMV Secure eSolutions, donde ha desarrollado su carrera profesional desde 1998. Ha sido premiado por la revista SIC (2012) por su trayectoria profesional y por Cloud Security Alliance (2015) e ISMS Forum (2013) por sus contribuciones en la Seguridad en Cloud Computing y en su estandarización. MBA por el Instituto de Empresa, es Ingeniero de Telecomunicaciones por la Universidad de Valladolid y cuenta con las certificaciones CGEIT, CISM, CISA y CRISC, por ISACA, CISSP por (ISC)2, e ISO 27001-LA y BS 25999-LA. En GMV, es responsable de su Sistemas de Gestión de Seguridad de la Información (ISO 27001, desde 2004) y de Continuidad de Negocio (ISO 22301, desde 2010).

López Bernal, Pedro Pablo, Gerente GRC & PIC (Compliance) de Rural Servicios Informáticos, Servicios Outsourcing Global, 1986, a CAJAS RURALES, Empresas Participadas y otros CLIENTES, más de 60 Entidades Financieras y Seguros. Técnico Informático, Máster Auditoria Informática 1991, CISA y Máster en Seguridad Global 2006, Primera Edición Curso Superior Infraestructuras Críticas GET/ UNED / Instituto Gutiérrez Mellado y Profesor del mismo. Los últimos 34 años trabajó en: ENTEL (hoy INDRA), CITIBANK, BANCO SANTANDER y RSI. Diversos puestos y funciones TIC (Auditoría, Seguridad, Riesgos, Continuidad, Calidad, Procesos, Sistemas, Fraude, Compliance, Infraestructuras, Privacidad, Gobierno, Resiliencia). Participa Comités, Foros, Grupos y Comisiones: Continuidad, Riesgos, Seguridad, Auditoria,

Fraude, Privacidad, Gobierno y Calidad, pionero Lucha contra el Fraude Online en España desde 2004 en CCI, Continuidad en CECON desde 2007, Grupo Ciberseguridad de IBERPAY, Seguridad y Continuidad de REDSYS y Grupos de Normalización de UNE/AENOR.

Miembro fundador Instituto Continuidad Negocio Español (CONTINUAM) y Observatorio Seguridad Integral, Gestión de Emergencias y Continuidad Operativa (SIGECO), presidente de ambos desde 2015, miembro del Grupo Regulación y de Seguridad AUTELSI, miembro de Comisión CON (Riesgos) ISACA, Comité Partes LEET Security. Presidente Comité de Seguridad Global, Jefe Emergencia RSI y miembro Comité Seguridad y Salud. Colaborador en Grupos y Publicaciones como: SIC, Red Seguridad, Computerworld/IDG, Computing, ISMS, IFAES, IKN, …

Lozano Merino, Marco Antonio, Ingeniero de software y Diplomado en tecnologías de la Informática por la Universidad SEK. Cuenta con una amplia carrera en el área de la ciberseguridad desempeñando tareas como asesor y consultor tecnológico desde hace más de 17 años en empresas de diversos ámbitos que discurren desde los medios de prensa hasta la Administración Pública. En la actualidad forma parte del elenco de expertos en ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), forma en diversos másteres de ciberseguridad y colabora con la Comisión Europea y diversos medios de comunicación. Cuenta con una amplia formación y certificaciones como CISM, GIAC, CCS-G, CCS-T, ITIL e ISO 27000 entre otras."

Montalbán Carrasco, Rocío, CIO del Ministerio de Justicia (Junio 17 - Actualidad) y anteriormente Subdirectora General Adjunta de Tecnologías de la Información y las Comunicaciones en el Ministerio de Industria, Energía y Turismo (Febrero 09 - Junio 17). Ingeniera Superior de Telecomunicación por la Universidad de Cantabria. Executive MBA por el Instituto de Empresa. Es funcionaria del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración General del Estado. Miembro, durante varios periodos, de la Junta Directiva de la Asociación profesional del citado cuerpo. Previamente ha desarrollado diversos puestos de responsabilidad en la Empresa Privada, especialmente en el sector de Consultoría y Telecomunicaciones.

Ortiz González, Ramón, Ingeniero Técnico Informática Gestión UPM, CISA, CISM por ISACA; PA Compliance en el IE, Master en Dirección de eCommerce y Marketing Digital por FED, Certified Cyber Security Professional por ISMS Forum Spain. Ha desempeñado cometidos en diferentes empresas como Tragsa, en proyectos de control por teledetección, proyectos de banca a distancia en diferentes entidades (Caja Ahorros de Navarra, Argentaria, SolBank-Sabadell) y en proyectos para la Administración Publica. Desde 2006 es el Responsable de Seguridad de Mediaset, con responsabilidad sobre la Ciberseguridad de los Sistemas IT y Broadcast. Miembro de la Unidad corporativa de Mediaset de Privacidad de los Datos, entre otros cometidos. Adicionalmente colabora en desarrollar e impartir sesiones de concienciación sobre Ciberseguridad y Privacidad a los empleados de las empresas del grupo. Miembro de grupos de trabajo en ISMS Forum y AUTELSI y colabora habitualmente como ponente en foros sectoriales de Ciberseguridad.

Pérez San-José, Pablo, Gerente de Ciberseguridad de Deloitte. Cuenta con más de 17 años de experiencia profesional en empresas como GfK, BBVA, INCIBE, Red.es, CNMC e ICEX. Ha dirigido y participado en proyectos de asesoramiento en la estrategia, organización y mejora de las capacidades de ciberseguridad para distintos organismos públicos y empresas, así como en numerosas investigaciones en seguridad, privacidad y confianza digital para el BBVA Global Observatory, el Observatorio de la Seguridad de la Información de INTECO, el Observatorio de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) o el Grupo de Análisis y Prospectiva de las Telecomunicaciones (GAPTEL) de Red.es, entre otros.

Picazo Zofio, Rafael, su carrera profesional se ha desarrollado en CLH, los puestos más relevantes han sido jefe de soporte técnico y comunicaciones, subdirector de gestión de aplicaciones y, el último, CISO.

Rubio Donis, Enrique, Ingeniero Industrial por la Universidad Politécnica de Madrid, Master's Certirficate in Project Management por la Escuela de Negocios de la George Washington University, cuenta con una amplia formación y experiencia en el gobierno de las tecnologías de la información. Ha desempeñado diferentes puestos de responsabilidad en Canal de Isabel II, siendo su puesto actual el de Jefe de Área de Planificación, Control y Seguridad de los Sistemas Informáticos, desarrollando funciones relacionadas con el gobierno de los sistemas de información y la seguridad de la información, siendo así mismo responsable de la oficina de soporte a la continuidad de negocio corporativa.

Santos García, Rafael L., Responsable del Área TIC en el Comisionado para el Mercado de Tabacos. Jefe de Área de Seguridad Informática/CISO del Ministerio de Fomento desde hace 4 años. Funcionario de carrera del Cuerpo Superior de Tecnologías de la Información y las Comunicaciones desde 1992. Ha ocupado puestos en diversos Organismos y Ministerios de la AGE en temas relacionados con la Seguridad Informática recibiendo para ello formación específica en Centros de la Administración y en Empresas y Universidades: (PIC – Programa en Innovación en Ciberseguridad – Curso de Postgrado – Universidad de Deusto.)

Aprovechamos también para agradecer a Aiuken, DXC y everis an NTT DATA Company por patrocinar el webinar en el que se presentó este estudio y el apoyo institucional de INCIBE en la celebración de este evento.

1 Introducción sobre la problemática de los Insiders

Centrarnos en el origen.

En ocasiones nos olvidamos de un hecho esencial en la ciberseguridad: la información junto con las personas conforma los principales activos de la compañía.

Con ese foco y atendiendo a las relaciones que, en las compañías, sea cual sea su tamaño, se establecen entre personas e información a través de los procesos y en ocasiones de las herramientas, es esencial identificar quién tiene acceso a la información y con qué grado de acceso y privilegios la trata. Esa actividad, adolece en muchos casos de un principio fundamental: <<la necesidad de conocer>>. Este principio, expresa la necesidad de acceso con privilegio mínimo a la información para conocer aquello que se necesita formalmente para desempeñar la actividad asociada a la función de la persona (usuario, trabajador, directivo, entre otros).

Es habitual encontrar en las corporaciones, empresas u organismos que los privilegios que se otorgan de acceso son en realidad un conjunto de permisos que no responden a un rol sino que o bien vienen heredados de funciones anteriores de la persona e incluso agregadas de otras funciones, necesidades puntuales o bien, responde al principio de mínima resistencia (a más privilegios de acceso, menos incidencias); lo que nos lleva a un escenario de riesgo de incidentes relacionados con la confidencialidad, disponibilidad e integridad, de la información

Este escenario, no es nuevo, pero hay una serie de factores internos y externos que nos obligan a reflexionar sobre: información, personas y privilegios.

Factores que, en este momento, nos llevan a la reflexión. Contexto.

Los principales, los encontramos en aspectos tales como: la mayor exigencia regulatoria y de cumplimiento, la inserción de la Tecnología en el ADN del Negocio, el empuje de las Ciberamenazas, que ya no son vistas como una rareza o exclusiva de las grandes empresas, sino que forman parte de la agenda de los ciudadanos, empresas de cualquier sector y tamaño, así como de la necesidad de “industrializar la defensa”.

Estos ataques han utilizado como vectores de entrada y como herramientas, una peligrosa triada.

- El factor humano. En este caso, la fragilidad de la cultura en materia de seguridad de los empleados, explotada a través de correos malintencionados.

- Las autorizaciones de acceso de los mismos a la información (así como al resto de activos TIC) o de otras personas que se vean implicados a través de los movimientos laterales.

- La facilidad de disponer de un malware potente de una forma fácilmente asequible. El cual, es adquirido por las redes de delincuentes como si se tratase de <<software comercial>>.

- La debilidad de las organizaciones frente a una vía en la que se invierte el 4% del presupuesto de seguridad y sin embargo en el que se generan el 87% de los incidentes de seguridad. Nos referimos al correo.

Desde finales del año pasado, hasta la fecha de publicación de este estudio, se vienen produciendo una serie de ataques que tienen como objetivo la información, que ponen en peligro no ya las operaciones de la empresa que ha sido víctima, sino también de aquellas que las han contratado o del sistema al que dan cobertura (como por ejemplo, el caso de un ataque ciber que puso en riesgo la disponibilidad de moneda acarreada en transportes de fondos).

El gran número de eventos de seguridad, de incidentes, requieren de una optimización de los esfuerzos de protección. Una de las vías para optimizar los esfuerzos, la encontramos en la modelización del comportamiento de personas y objetos; es decir, debemos centrar la atención en aquello que se sale de lo normal.

Por todo ello, necesitamos perfilar el acceso a la información mediante la definición de roles y perfiles que se adapten a las necesidades de "conocer" de cada puesto y función.

El grupo de trabajo de Calidad y Seguridad identificó la necesidad de reflexionar sobre las diferentes necesidades funcionales de acceso a la información y en consecuencia de los privilegios con los que tratan la misma y las medidas de seguridad que deberían aplicarse a cada rol, durante todo el ciclo de vida de la relación de la persona con la empresa.

Hablamos por tanto de identificar que controles de seguridad Organizativos, administrativos y técnicos aplican a cualquier persona que tiene una relación directa con la empresa; los conocidos como Insider.

1.1 Objeto del análisis: definición de insider.

Definición del término.

El término *insider* (proviene del inglés y literalmente quiere decir "el que está dentro") se refiere a la persona o personas que, debido a su posición dentro de una corporación, normalmente en posiciones especiales (órganos de dirección o administradores de sistemas (por mencionar dos casos ilustrativos), le permitan tener conocimiento de información confidencial o privilegiada.

La definición anterior es una "versión" sencilla, de la que manejaremos como referencia:

El término insider se refiere a cualquier persona que de forma intencional, a través de una acción concreta o por omisión de su acción, ya sea de forma directa, indirecta o en connivencia

con terceros (internos o externos a la organización) pueda influir de forma negativa o causar un impacto o daño en la seguridad como la reputación y, en especial, en la seguridad y privacidad de la información, independientemente de si su acción u omisión causa su efecto durante su relación y estancia "in situ" o de forma remota, así como durante una relación contractual con la organización o una vez extinguida aquella.

Causas, motivaciones y daños asociados a las actuaciones negligentes o intencionadas de los insiders.

1. **Trabajador Descuidado** (uso impropio de activos). Empleados o socios que se apropian indebidamente los recursos, violan políticas de uso aceptables, manejan mal los datos, instalan aplicaciones no autorizadas y usan soluciones alternativas no aprobadas; sus acciones son inapropiadas en lugar de maliciosas (no hay intencionalidad de hacer daño), muchas de las cuales entran dentro del mundo de Shadow IT (es decir, fuera del conocimiento y la administración de TI).

2. **Agente Interno** (robar información en nombre de terceros maliciosos). Insiders, reclutados, extorsionados o sobornados, por terceros para exfiltrar datos.

3. **Empleado descontento**. Personas internas que buscan dañar su organización a través de la destrucción de datos o la interrupción de la actividad empresarial.

4. **Insider malicioso** (robar información para el beneficio personal). Actores con acceso a activos corporativos que utilizan sus privilegios para acceder a la información con fines de lucro personal.

5. T**erceros** (comprometiendo la seguridad). Socios comerciales o contratados, que comprometen la seguridad mediante negligencia, mal uso o acceso malintencionado o uso de un activo.

Caracterización.

Las brechas con exfiltración / daños a los activos de información causados por insiders malintencionados , tienen una serie de características que las hacen especialmente dañinas:

- Conocimiento del valor de los activos (especialmente de la información).

- Capacidad de disimular las acciones malintencionadas con las propias del desempeño de la función.

- Persistencia o dificultad temporal para ser descubiertos.

En relación a la última de estas tres características, es muy interesante el grafico que el estudio “Insider Threat Report Out of sight should never be out of mind” de la Empresa Verizon.

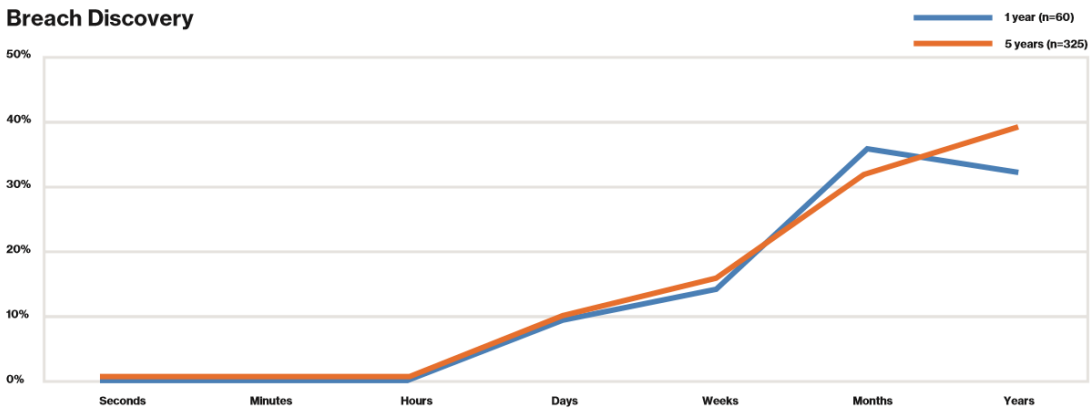

Figure 3.
Breach Time to Discovery within Insider and Privilege Misuse Breaches

1.2 Destinatarios y objetivos del estudio

A quién va dirigido este Estudio

Este Estudio va dirigida tanto al sector público como al sector privado español con independencia del tamaño o sector de actividad de la empresa.

Respecto a los perfiles a los que nos dirigimos son:

- Principalmente, a la persona o puesto, en el desempeño de la función de Responsable de la seguridad de la información, o CISO, dado que es en ámbito dónde típicamente se definen y supervisan e incluso se implantan, las medidas de prevención y protección, las cuales pueden incluir la gestión de las identidades y accesos a la información, por los diferentes actores del entorno del negocio.

- Adicionalmente, a Auditores y miembros de Compliance, pueden encontrar también información útil para el desempeño de su función.

Función del Estudio

La función de la presente guía es dar soporte a los profesionales de la seguridad de la información y responsables en esta materia para que puedan abordar esta problemática en sus diferentes situaciones, con un criterio homogéneo y contrastado, siguiendo una serie de buenas prácticas.

Esta Estudio también pretende servir de elemento de sensibilización y de acercamiento de dicha problemática a los distintos órganos de Dirección de las empresas y organismos públicos.

Objetivo del Estudio

Se pretende que este documento sea eminentemente práctica y breve para que pueda cumplir con su objetivo que es: ayudar a identificar e implantar de manera rápida y eficaz los controles

y medidas adecuados para prevenir y mitigar los riesgos de seguridad asociados en cada caso a los diferentes perfiles de insiders en las organizaciones.

- Identificar los diferentes roles y sus correspondientes posiciones en la organización, asociados al término insider.
- Identificar los controles de seguridad, a lo largo de todo el ciclo de vida de la relación del insider con la empresa, que conforman las buenas prácticas que le son de aplicación.
- Destacar aquellos controles que o bien son específicos o se emplean de forma reforzada para roles relevantes de los insiders.

2 Metodología de trabajo (reuniones comunes, trabajo por grupos de expertos…)

El Grupo de Ciberseguridad y Privacidad de AUTELSI ha identificado como del máximo interés para los asociados la elaboración de un "**Estudio sobre los Insiders".**

El grupo de trabajo está constituido por profesionales de avalada y dilata experiencia, en diferentes campos de especialización; responsables de seguridad, auditores, gestores de Riesgo, jurídicos, consultores, desarrolladores de negocio, tecnólogos, entre otros.

La metodología para elaborar esta guía ha consistido en responder a las preguntas que las organizaciones se plantean cuando se enfrentan a la problemática de los insiders: quiénes son, en qué ciclo de vida de su relación con la organización y qué controles instauran y medidas implantar para prevenir y mitigar el impacto de los riesgos de seguridad derivados de su presencia en la organización y acceso a los sistemas y la información de la misma y, por ello, la posibilidad de un incidente de seguridad asociados a los mismos.

Para elaborar las respuestas, se han creado varios subgrupos de trabajo, enfocados en el estudio de cada uno de los perfiles identificados.

Posteriormente se han revisado colectivamente, los resultados de los subgrupos.

Finalmente, el equipo de coordinación ha revisado nuevamente los resultados y ha editado el contenido definitivo.

3 Identificación de los 13 perfiles de insider y su caracterización

El grupo de trabajo ha identificado un total de 13 perfiles, los cuales corresponden tanto a personal interno (seis) como a personal externo (7):

3.1 Personal interno

1) Puestos sensibles con autorización permanente para acceder a toda la información sensible o confidencial
2) Puestos sensibles con autorización permanente para acceder a una específica y concreta información sensible o confidencial
3) Puestos sensibles con autorización permanente para acceder a una específica y concreta información sensible o confidencial
4) Puestos para acceder específicamente a una información sensible
5) Puestos con autorización permanente para acceder a una específica y concreta información pública, sensible o confidencial
6) Puestos que si acceden a la información sería por un fallo en el sistema o por violación de la política de seguridad

3.2 Personal externo

7) Puestos sensibles con autorización permanente para acceder a información, sensible o confidencial, especifica
8) Colaboradores (no proveedores)
9) Stakeholders relevantes
10) Personal externo administrador
11) Personal externo supervisor
12) Usuarios externos/clientes
13) Puestos que si acceden a la información sería por un fallo en el sistema o por violación de la política de seguridad

Sumariamente, en la siguiente tabla se expresan el perfil, en base a si es Personal interno o externo, el “alcance organizativo” de su función, a si accede a una parte (de forma limitada a una información específica) o a la totalidad de la información del alcance organizativo (empresa, departamento,), si es el propietario o no de la información y el modo en el que lo hace (consulta o Edición).

ID	Puestos (ejemplos)	Perfil	Personal	Nivel de Información	Ámbito (extensión) de la información	¿Es el propietario de la información?	Modo
Id 1	Presidente, Consejo, Dirección y Mandos de departamentos Financiero, Auditoria, Jurídico, Seguridad, Privacidad, Riesgos, Continuidad, RRHH	Puestos sensibles con autorización permanente para acceder a toda la información sensible o confidencial	Interno	en toda la estructura o en ciertas áreas de la Compañía	Toda	NO	Consulta
Id 2	Secretarias, Personal de departamentos Financiero, Auditoria, Jurídico, Seguridad, Privacidad, Riesgos, Continuidad, RRHH	Puestos sensibles con autorización permanente para acceder a una específica y concreta información sensible o confidencial	Interno	en ciertas áreas de la Compañía	Especifica	SI	Edición
Id 3	Administradores de sistemas y herramientas (superusuarios), Dpto informático (mantenimiento)	Puestos sensibles con autorización permanente para acceder a una específica y concreta información sensible o confidencial	Interno	en ciertas áreas de la Compañía	Especifica	NO	Consulta
Id 4	SOC/CERT propio, forense interno, control interno, auditoria interna)	Puestos para acceder específicamente a una información sensible	Interno	en toda la estructura o en ciertas áreas de la Compañía	Especifica	NO	Consulta
Id 5	Usuarios (empleados, becarios, t. en prácticas) de la información	Puestos con autorización permanente para acceder a una específica y concreta información pública, sensible o confidencial	Interno	en ciertas áreas de la Compañía	Especifica	NO	Edición

Id 6	Usuario o atacante interno	Puestos que si acceden a la información sería por un fallo en el sistema o por violación de la política de seguridad	Interno	-	NA	NO	NA
Id 7	Proveedores en general y personal externo que presta servicios a departamentos Financiero, Auditoria, Consultoría,Jurídico, Seguridad, Privacidad, Riesgos, Continuidad, RRHH… Con especial atención a subcontratistas, factorías SW, servicios profesionales (Jurídicos, Gestores, Consultores, etc.), Auditores, ETT, Headhunters,…	Puestos sensibles con autorización permanente para acceder a la información, sensible o confidencial , especifica	Externo	en ciertas áreas de la Compañía	Especifica	NO	Edición
Id 8	UTEs, socios de negocio, socios tecnológicos	Colaboradores (no proveedores)	Externo	en ciertas áreas de la Compañía	Especifica	SI	Edición
Id 9	Accionistas, Inversores institucionales Inspectores, Reguladores	Stakeholders relevantes	Externo	en ciertas áreas de la Compañía	Toda	NO	Consulta
Id 10	Administradores de identidades, equipos, redes sistemas o bases de datos	Personal externo administrador	Externo	en ciertas áreas de la Compañía	Especifica	NO	Consulta
Id 11	proveedores y personal externo que presta servicios de seguridad, forense, CERTs, auditores externos, inspectores	Personal externo supervisor	Externo	en ciertas áreas de la Compañía	Especifica	NO	Consulta

Id 12	Clientes, usuarios externos	Usuarios externos/clientes	Externo	en ciertas áreas de la Compañía	Especifica	NO	Edición
Id 13	Usuarios o atacantes externos	Puestos que si acceden a la información sería por un fallo en el sistema o por violación de la política de seguridad	Externo		NA	NO	NA

4 Identificación de los 6 “momentos” a lo largo del ciclo de vida del insider.

Los controles no sólo dependen de la función sino también y como es lógico del momento en el que se encuentre dentro del ciclo de vida de la relación contractual del insider con la empresa. A tenor de ello se identifican, los diferentes estados de dicha relación:

1) Antes de la Contratación
2) Durante la Contratación
3) Inmediatamente tras la contratación
4) Periódicamente durante el contrato
5) En caso de Cambio de Puesto
6) Tras causar baja en la empresa

5 Tipología de controles (administrativos, técnicos…)

Los miembros del grupo, de forma individual y posteriormente a través de los subgrupos y finalmente a través de la revisión conjunta del grupo, han seleccionado un conjunto de controles y con toda la anterior información de los apartados anteriores, se ha determinado para los diferentes perfiles, los controles que les serán de aplicación, junto con el momento de la relación contractual en el que debe ser aplicado.

En las tablas finales, por una cuestión de espacio y legibilidad el perfil es referenciado por su ID (del apartado 3).

Tras varias revisiones, el grupo concluyó, que, con matices, hay un conjunto de controles que se aplican a todos los perfiles y un subconjunto menor o bien son específicos o bien tienen especial importancia en un tipo de perfil.

Debe entenderse, que hay muchos más controles que los que se mencionan en nuestras tablas, pero o bien corresponden más a una infraestructura, en lugar de estar relacionados con las personas que manejan la información o bien no nos resultaron relevantes.

Finalmente indicar, que por estos motivos esta relación no es exhaustiva, sino que responde a lo que creemos es una aproximación que aporta reflexión y pautas de refuerzo de controles.

5.1 Controles/medidas globales comunes para todos los perfiles.

En la primera hoja de cada tabla se muestran los controles comunes (con matices) a todos los perfiles.

Para cada uno de los perfiles hay una tabla con todos los controles que le serían de aplicación dentro del alcance del presente trabajo.

5.2 Medidas específicas para cada perfil.

A título de ejemplo hemos desarrollado cuatro de estos perfiles de una forma explicativa para una mejor compresión.

Cada uno de ellos se explican no con una misma estructura común para los cuatro, dado que hemos preferido mantener los diferentes enfoques que los subgrupos han dado a estos ejemplos, a fin de poner de manifiesto que la forma de acercarse los profesionales a un mismo problema, puede ser diferente y por tanto más enriquecedor el resultado.

6 En detalle, cuatro casos de uso paradigmáticos

Estos son los cuatro perfiles elegidos; dos de personal interno y dos de personal externo

- Personal interno:
    - Caso A: Alta dirección VIP (Perfil 1)
    - Caso B: Empleados con permisos privilegiados (Perfil 3)
- Personal externo
    - Caso C: Personal externo / personal subcontratado (Perfil 7)
    - Caso D: Inspectores, auditores, reguladores (Perfil 9)

6.1 Personal interno:

Caso A: Alta dirección VIP (Perfil 1)

Puestos sensibles con autorización permanente para acceder a toda la información sensible o confidencial

Se encuentran en este caso, Presidencia, Consejo de Administración, Comité Ejecutivo, Altos Cargos de la Administración y del Gobierno, Departamento Financiero, Seguridad, Privacidad y Recursos Humanos

Para describir la tipología de riesgo que presenta este perfil, lo haremos desde tres enfoques diferentes: Como objetivo de ataques, como amenaza no intencionada y como modelo de comportamiento:

En el enfoque del perfil 1 como objetivo de ataques consideramos:

- Que los altos directivos tienen una frecuente presencia pública, que les hace tener que trabajar y conectarse desde ubicaciones remotas, tales como hoteles, aeropuertos, y otros tipos de espacios públicos o privados, fuera del perímetro corporativo. Esto les hace más vulnerables a determinadas tipologías de amenaza.
- Los hackers van a dirigir sus ataques de manera selectiva contra estos altos directivos, ya que son ellos los que manejan información sensible y privilegiada, información que en manos de los hackers puede tener mucho más valor que las informaciones que manejan otros perfiles de usuarios.
- Además, los hackers que tienen como objetivo a los altos ejecutivos están dispuestos a invertir más tiempo y ser más pacientes, en sus intentos, hasta que encuentran la situación de vulnerabilidad.

Por otra parte, en el enfoque de amenazas no intencionadas nos encontramos con:

- Ataques de phising para robo de credenciales, a los que el ejecutivo puede ser más vulnerable, ya que la gran presión a la que están sometidos por procesar información y tomar decisiones con gran rapidez, dificulta dedicar el tiempo a analizar la legitimidad de un correo o de una comunicación.

- Extravío de un dispositivo móvil en el que se ha accedido a información sensible, o almacenamiento de esa información en un dispositivo externo o un cloud privado.

- Almacenamiento de claves de acceso en cualquier medio físico o electrónico.

Y finalmente y de gran transcendencia es el rol del alto directivo como sponsor:

- Si los ejecutivos no son los primeros en adoptar todas las prácticas y políticas de seguridad, los empleados que dependen jerárquicamente de ellos seguirán su ejemplo.

- Los ejecutivos deben recordar en cada reunión con sus equipos la importancia del respeto a las prácticas de seguridad, y deben preguntar regularmente por el estado de cumplimiento, formación de los empleados e incidencias abiertas.

- La asignación prioritaria de presupuestos para la seguridad y el posicionamiento adecuado del CISO y el responsable de riesgos en el organigrama son también una responsabilidad del alto directivo para garantizar el cumplimiento de las prácticas de seguridad por todos los empleados.

Es por todo ello que es especialmente relevante para este colectivo la correcta aplicación de los controles técnicos de autenticación y acceso de usuarios, el cifrado y protección de la información, y una respuesta rápida a incidentes, de cara a reducir su nivel de exposición y vulnerabilidad.

Caso B: Empleados con permisos privilegiados (Perfil 3)

Personal interno, Empleados con permisos privilegiados.

El perfil 3, analizado en este estudio, se refiere los usuarios Administradores de Sistemas y arquitecturas de las compañías.

Sin ánimo de agotar a qué recursos corporativos tienen total acceso este tipo de perfiles, podríamos mencionar:

Equipos locales, servidores físicos y virtuales, servicios, dominios, bases de datos, aplicaciones, arquitectura de red y de comunicaciones, sistemas de respaldo y registro de la información, infraestructura de suministros esenciales y accesos físicos y gestión de alertas y emergencias.

Entendiendo por total acceso a la capacidad de los empleados de este tipo de acceder a la información, inclusive de manipularla, cambiar configuración de equipamiento y arquitecturas, modificar o anular temporal o definitivamente las salvaguardas de auditoría, de control y hasta el cifrado sobre la información, configuración y acceso a los recursos corporativos, independientemente del tipo que sea.

Es decir, y con poco margen para otras interpretaciones, nos encontramos ante un perfil, que su mala praxis de modo deliberado, o por coacciones por parte de terceros, puede tener consecuencias catastróficas para los intereses de la empresa. Añadamos además que es frecuente que estos perfiles son desempeñados por personal externo (tratado en otro apartado del estudio), otra "variante" de perfiles privilegiados es la existencia de credenciales con amplias facultades de acceso utilizadas por servicios o scripts, las cuentas impersonales.

Adicionalmente a lo ya expuesto y para acrecentar aún más las acciones de este tipo de perfiles, en ocasiones, desgraciadamente la actividad de estos empleados con permisos privilegiados se realiza por medio de credenciales genéricas y que son utilizadas por un número indeterminado de usuarios, impidiendo tal y como es preceptivo atribuir las operaciones realizadas a un individuo concreto.

Todo lo comentado anteriormente pinta un panorama desolador, si bien en términos generales, este riesgo a menudo no es categorizado en los análisis de riesgo como alto, ni se le dedican controles y medidas, que están descritas extensamente y son accesibles y aplicables.

En ocasiones esta falta de tratamiento es por dudas e indecisiones sobre en qué área deberá recaer el control de estos colectivos.

En el análisis realizado, al perfil de usuarios de cuenta privilegiada, y como ya se verá, le aplican prácticamente todos los controles y tipologías de los mismos redactados por el grupo de trabajo de insiders.

El enfoque positivo sobre esta cuestión es la inclusión legislativa de la responsabilidad de la empresa en la gestión de riesgo en tratamientos de datos de carácter personal, y gestión de los activos de información, infraestructuras críticas, etc. en donde la adopción de normativas y buenas prácticas reconocidas facilitan el cumplimiento e inciden en la adopción de medidas sobre la acción de estos colectivos. Comentar además que existen en el mercado productos de fabricantes muy maduros que proporcionan la adopción de técnicas y medidas de almacenamiento y rotado de contraseñas de cuentas privilegiadas, grabación de sesiones de administración, etc.

6.2 Personal externo

Caso C: Personal externo / personal subcontratado (Perfil 7)

Personal Externo: Perfil 7 - Subcontratas

Hoy en día las Compañías demandan cada vez más servicios profesionales subcontratados que implican la incorporación insitu o de forma remota de personal externo.

Este personal externo requerirá de acceso a los sistemas de información de la Compañía para poder llevar a cabo las operaciones para las cuales se le ha contratado. Estas operaciones pueden ser de todo tipo, y el acceso puede ser a cualquier sistema y por tanto, a cualquier información (más o menos confidencial).

Lo que tienen que tener en cuenta las compañías es que el perfil del subcontratado (personal externo) tiene un ciclo de vida diferente al del personal interno, y que por tanto se han de tener en cuenta diferentes consideraciones a la hora de incorporar dicho perfil.

Previo a la contratación: Hay que asegurarse que a nivel contractual se han tenido en cuenta, y por tanto se han firmado, todas las cláusulas de confidencialidad y de protección de datos aplicables a la prestación del servicio por la empresa subcontratista.

Durante la prestación del servicio: Todo personal externo debe tener un responsable interno que asegure que la gestión de los accesos sea la correcta. Esta gestión implica el alta y la modificación de los permisos en los sistemas de información corporativos.

- Alta: asegurarse que el usuario externo es dado de alta en los sistemas de información necesarios y con los permisos adecuados.
- Modificación: asegurarse que durante toda la prestación del servicio, el usuario externo dispone de los accesos adecuados, tanto a nuevos sistemas si hay nuevas necesidades, como revocando accesos si ya no son necesarios.

Al finalizar la prestación del servicio: hay que asegurarse que una vez finaliza la misma por parte del trabajador externo, se revocan todos los accesos y se da de baja al usuario de los sistemas de información. De igual forma hay que asegurarse que una vez finalizada la prestación del servicio, el subcontratista entrega toda la información procesada durante la misma garantizando la integridad de la información.

A continuación, un ejemplo:

Una multinacional contrata a un proveedor especialista en analítica de datos para llevar a cabo un proyecto de Big Data. El proyecto va a durar 5 meses y van a trabajar en él 4 consultores externos. La multinacional asigna a un Jefe de Proyecto interno que liderará el mismo y se asegurará del cumplimiento de los hitos del proyecto.

Se ha firmado un contrato en el que se han incluido todas las cláusulas de seguridad, así como de confidencialidad y de protección de datos de carácter personal, ya que se van a tratar datos de clientes.

El jefe de proyecto tiene que solicitar acceso para los 4 consultores a los sistemas de información implicados en el proyecto con acceso de lectura a los datos. Si durante el proyecto surge la necesidad de integrar algún sistema adicional, los consultores solicitaran acceso al mismo a través del jefe de proyecto.

Una vez finaliza el proyecto y se cumple con los entregables del mismo, el jefe de proyecto solicitará la baja de los sistemas para los 4 consultores externos y se asegurará que se entregan todos los datos que se hayan utilizado en el transcurso del proyecto.

Caso D: Inspectores, auditores, reguladores (Perfil 9).

Personal externo: Perfil 9-Stakeholders relevantes

El término "*stakeholder*" fue ampliamente divulgado mediante su aparición en el libro *Strategic Management: A Stakeholder Approach* (1984) por R. Edward Freeman. La ISO 26000 define a los *stakeholders* o "*partes interesadas*" como "Individuo o grupo que tiene interés en cualquier decisión o actividad de la organización". Según esta definición, se trata de aquellas personas que, por distintas razones, tienen interés en la existencia, estrategia, objetivos y desarrollo de una empresa. Su grado de interés dependerá del impacto que tengan las decisiones de la empresa en ellos y viceversa. Los *stakeholders* poseen los atributos de legitimidad, poder de influencia y urgencia.

Como primer paso identificaremos los *stakeholders* que pudieran relacionarse con nuestra organización. Algunos ejemplos son: accionistas, competidores, proveedores, inversores, acreedores, socios, clientes, trabajadores, organismos reguladores, inspectores, auditores, medios de comunicación, sindicatos y usuarios.

Por sus propias características y modos de conducirse dentro de la Compañía, los controles objeto de este estudio de *insiders* que le son aplicables a este perfil tienen determinadas limitaciones o particularidades, en cuanto a su ciclo de vida y tipo de control. Se tendrán en cuenta durante la relación con la organización, así como una vez finalizada, pero no en momentos anteriores. El ámbito de información al que tienen acceso es total, pero en ciertas áreas de la organización, y será de tipo consulta y revisión.

En general, los controles de tipo técnico aplicables al resto de *insiders*, tanto internos como externos, serán de aplicación sólo en aquellos casos en los que los *stakeholders* utilicen, de forma directa, activos y herramientas de la compañía gestionados corporativamente y en donde su actividad y rol como interesado sea efectivo. Como resumen, gestión de identidades, autenticación y permisos; control de acceso a instalaciones, a sistemas y servicios; gestión de soportes y dispositivos móviles; control técnico de la salida de información; etc.

De los controles de tipo administrativo, dada la naturaleza de la información a la que tienen acceso los *stakeholders*, relevante en cuanto a la dirección de la organización, les son aplicables todos aquellos relacionados con:

- La comunicación de las Políticas de Seguridad, confidencialidad, protección de datos, propiedad intelectual y *compliance*.
- Asignación de responsable interno para contacto y acompañamiento del *stakeholder*.
- Registro en la definición y asignación de accesos y privilegios cuando fuera necesario. Acceso a la definición de funciones y responsabilidades.
- Recolección de documentación y registros, acuerdos de confidencialidad.
- Involucración en la concienciación, gestión de cambios, estadísticas de actuaciones y auditoría de resultados.
- Capacitación de notificar incidentes y violaciones de las políticas y planes estratégicos, en cuanto a la información revisada.
- Entrega y devolución de la documentación de la organización. Destrucción de soportes e información cuando no se puedan devolver.

7 Reflexiones finales

Desde el Grupo consideramos que hemos alcanzado el objetivo que movía este trabajo de análisis. Por una parte, se han identificado y descrito los distintos perfiles de insider que pueden darse en las organizaciones; por otra parte, se han definido las etapas del ciclo de vida de la relación del insider con la organización; y finalmente, en función de cada etapa se recomiendan implantar unos controles y llevar a cabo una serie de medidas según cada perfil.

En este sentido, como segunda conclusión que apuntamos, es que además de señalar en cada caso el nivel y manejo de la información que requiere cada insider para desempeñar su función, es necesaria una responsabilidad activa de las empresas bien directamente, instaurando los controles necesarios en el marco del ejercicio del control de la actividad empresarial sobre los activos, sistemas, personas y recursos; bien de forma indirecta, exigiendo a aquellos en aquellos terceros (otras empresa so personas individuales) en quien se externalizan las funciones los tratamientos o los medios, que sigan estas mismas buenas prácticas. En cualquier caso, la supervisión de dichas exigencias forma parte de la propia diligencia debida como responsable último de la seguridad de la organización.

Una última conclusión es que las empresas deben realizar un ejercicio de identificación y clasificación de sus activos de información, privilegios de acceso y autorizaciones a los mismos, así como de los diferentes roles/perfiles funcionales (que deben ser definidos) , los cuales interaccionan en su entorno empresarial.

Si bien las amenazas de empleados sin escrúpulos o descontentos pueden ser inevitables, existen métodos para limitar el daño. Nuestra experiencia en investigación confirma las mejores prácticas de la industria para prevenir y mitigar las amenazas internas a través de una serie de principios:

- **Segregación de funciones**, especialmente para procesos y tareas sensibles o compartidas. Esto garantiza que ningún individuo pueda completar tareas que no puedan ser realizadas por una única persona (por ejemplo, una persona que solicite material y después sea la misma persona la que lo recepciona, chequea y paga).

- **Privilegio mínimo** Sólo asigne privilegios de acceso mínimamente necesarios para realizar una tarea. Esto limita las acciones no autorizadas o no deseadas. Asegúrese de que el acceso refleje los cambios de rol.

- **"Necesidad de saber"** Sólo conceda el acceso necesario para realizar un trabajo o función. Esto limita la exposición de datos y dispositivos confidenciales, como secretos comerciales, datos de clientes e información industrial o comercial.

Para evitar los daños no intencionados, recuerde trabajar el principio de **Conocimiento a través de la formación y la capacitación.** Este conocimiento se establece a través de:

- **La difusión de Políticas y Procedimientos**. Qué son y por qué se han definido. Redactelas de una forma sencilla y entendible. Revise todas las políticas de

ciberseguridad asociadas con los empleados, incluido el uso aceptable, BYOD, seguridad de la información y seguridad física.

- **Cultura de seguridad.** Cómo detectar los intentos de ingeniería social, cómo reconocer los indicadores de amenazas internas y cómo / cuándo informar de problemas de seguridad sospechosos.
- **Comportamiento aceptable del usuario.** Qué es y qué no es aceptable.
- **Consecuencias disciplinarias.** Cuáles son las consecuencias de actividades no autorizadas o maliciosas.

Sobre la base de este ejercicio de reflexión, atención y actuación, las empresas han de proponer y actuar en consecuencia, respaldados conforme una serie de buenas prácticas de seguridad, como las que este documento sugiere.

8 Fichas individuales para cada perfil (Tablas Excel)

Pulsando en cada uno de los perfiles puede descargar la tabla excel – ficha individual de cada perfil.

Personal interno

- **Perfil 1** - Puestos sensibles con autorización permanente para acceder a toda la información sensible o confidencial
- **Perfil 2** - Puestos sensibles con autorización permanente para acceder a una específica y concreta información sensible o confidencial
- **Perfil 3** - Puestos sensibles con autorización permanente para acceder a una específica y concreta información sensible o confidencial
- **Perfil 4** - Puestos para acceder específicamente a una información sensible
- **Perfil 5** - Puestos con autorización permanente para acceder a una específica y concreta información pública, sensible o confidencial
- **Perfil 6** - Puestos que si acceden a la información sería por un fallo en el sistema o por violación de la política de seguridad

Personal externo

- **Perfil 7** - Puestos sensibles con autorización permanente para acceder a información, sensible o confidencial, especifica
- **Perfil 8** - Colaboradores (no proveedores)
- **Perfil 9** - Stakeholders relevantes
- **Perfil 10** - Personal externo administrador
- **Perfil 11** - Personal externo supervisor
- **Perfil 12** - Usuarios externos/clientes
- **Perfil 13** - Puestos que si acceden a la información sería por un fallo en el sistema o por violación de la política de seguridad


autelsi