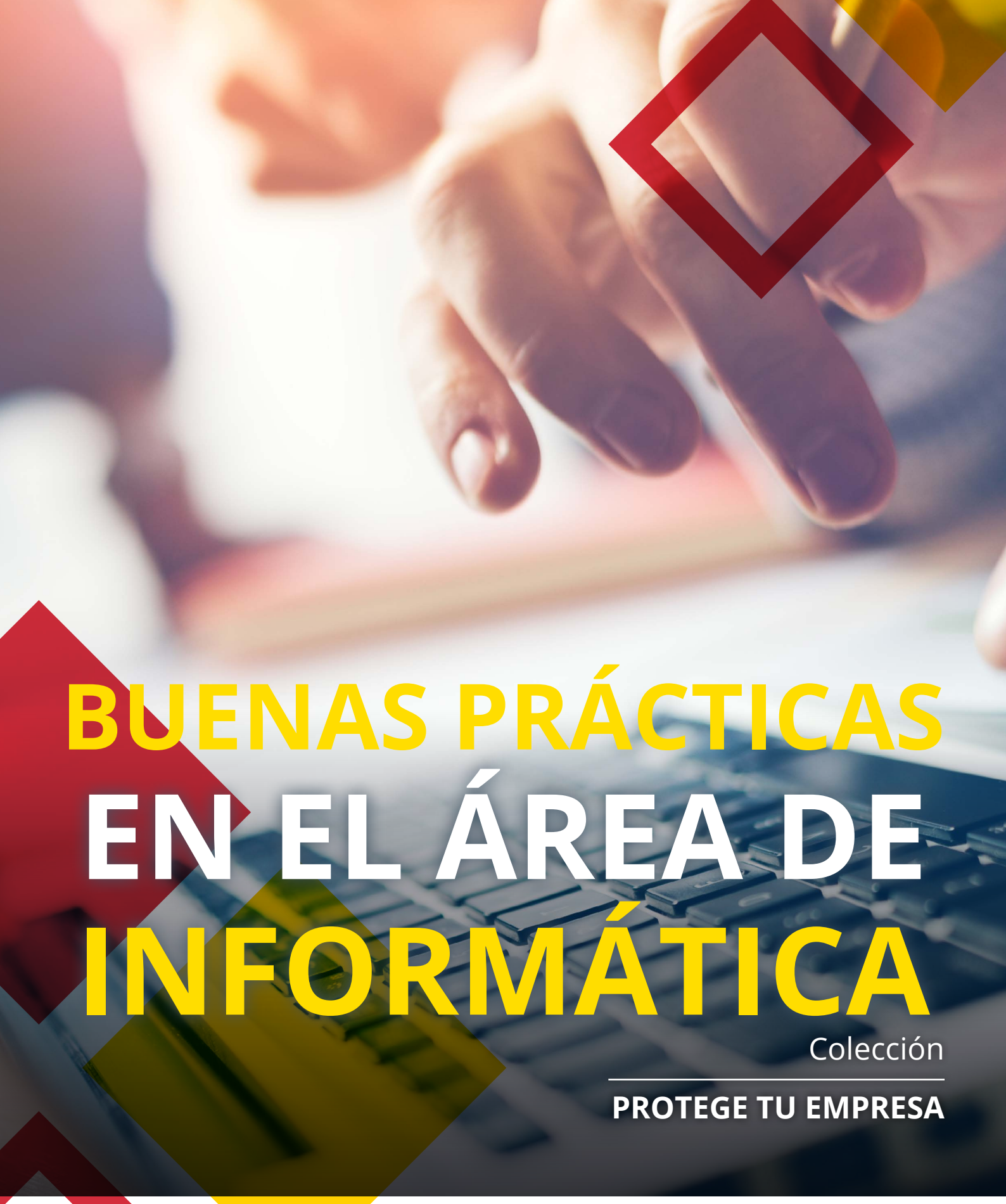


BUENAS PRÁCTICAS EN EL ÁREA DE INFORMÁTICA

Colección

PROTEGE TU EMPRESA

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ÍNDICE

ÍNDICE

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

Los avances tecnológicos en Internet, las redes, los dispositivos y la computación en la nube; junto a los servicios derivados de éstos como el comercio electrónico, la administración electrónica, los blogs, las redes sociales y las herramientas de colaboración, están transformando la forma de hacer negocios.

Las empresas basan su actividad en los **sistemas de información**, apoyando su gestión con los nuevos soportes tecnológicos. El uso masivo de estos sistemas para los negocios los convierte en el objetivo de los ciberdelincuentes, que aprovechan las vulnerabilidades de los mismos para acceder a ellos y desarrollar su actividad delictiva.

Es fundamental para la organización gestionar adecuadamente **la infraestructura tecnológica sobre la cual se sostiene nuestra información:** servidores, dispositivos de red, repositorios documentales, aplicaciones de gestión, sistemas de gestión empresarial, etc. El aumento de estos recursos tecnológicos ha desembocado en que su gestión sea considerada como uno de los pilares fundamentales, debido sobre todo, a la dependencia que el negocio tiene de las infraestructuras tecnológicas.

La mayoría de las organizaciones no disponen de un departamento de informática interno exclusivo para este fin. Por norma general, estos servicios son subcontratados a empresas externas para que realicen la gestión de la infraestructura tecnológica, convirtiéndose de esta forma en un departamento de informática externo. Estos departamentos, también conocidos como **departamentos de Tecnología de la Información** (TI), ya sean internos o externalizados, son parte del núcleo de las organizaciones y un aspecto vital para la eficacia y la eficiencia de nuestras operaciones. El avance reciente de las nuevas tecnologías ha contribuido a que actividades aparentemente tan poco tecnológicas como por ejemplo el reparto de paquetería, sea optimizada haciendo uso de: planificación de rutas, facturación e inventario en tiempo real durante el reparto o notificaciones de entrega vía SMS o correo electrónico.

A medida que nuestra dependencia tecnológica va creciendo, el departamento de **informática** cobra mayor relevancia, al ser el responsable de que los equipos y la información de la organización así como de protegerlos adecuadamente. Este departamento también tiene entre sus funciones aportar nuevas herramientas para mejorar el desempeño de nuestro trabajo, así como soluciones **[1]** para mejorar en la seguridad de la información y su tratamiento.

Es evidente, por tanto, que el mantenimiento y la gestión de la infraestructura tecnológica son necesarios para cualquier empresa que tenga dependencia de los activos tecnológicos y de la información en formato digital.

2. CLASIFICACIÓN DE LAS AMENAZAS

Las nuevas tecnologías han impactado de forma positiva en nuestras empresas pero, al igual que cuando éstas no existían, los riesgos a los que está expuesta la información se mantienen. Imaginemos, por ejemplo, un libro de contabilidad. Existe el mismo riesgo de pérdida de datos, extravío, robo, etc. para un libro «clásico» en papel que no custodiamos debidamente, como el que se encuentra en un fichero de datos dentro de nuestro ordenador portátil. Los medios cambian pero los riesgos continúan. Siguiendo una serie de medidas básicas de seguridad podemos reducirlos.

Nuestra empresa tiene información sensible como tarifas, márgenes de venta o datos personales de nuestros clientes, la cual debemos proteger frente a una serie de amenazas. Básicamente, podemos distinguir **entre amenazas externas e internas**, y en ambos casos, pueden ser **intencionadas o accidentales.**

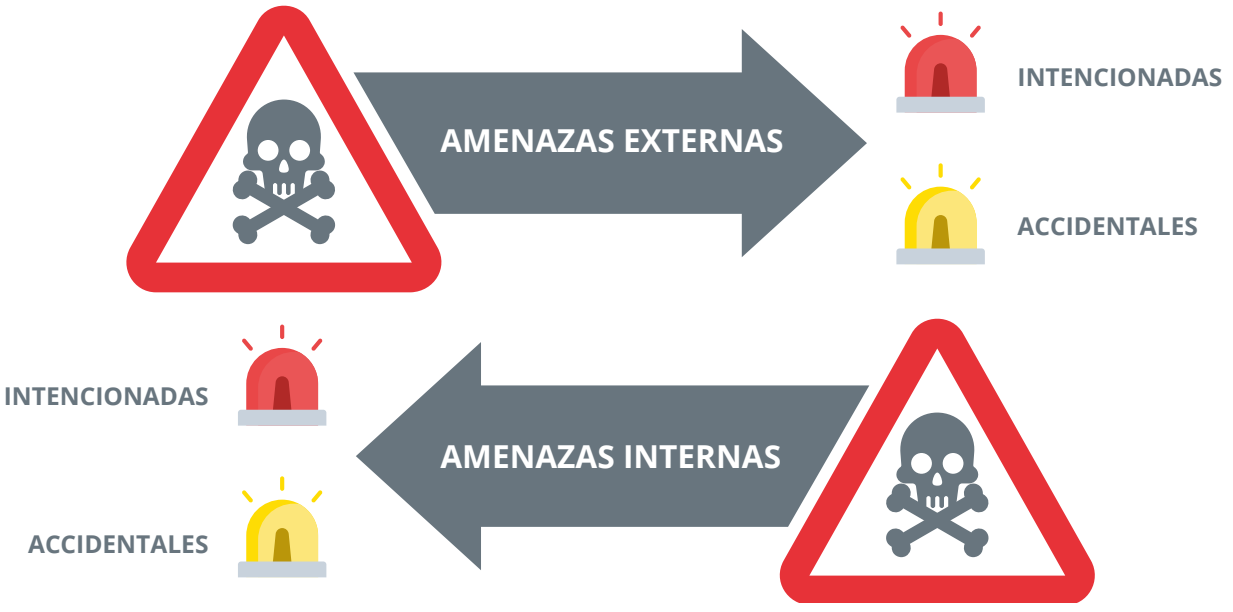


Ilustración 1
Tipos de amenazas

- **Amenazas externas intencionadas.** Espionaje, sabotaje, vandalismo, robo de información confidencial son algunas de las amenazas externas a las que nos enfrentamos. En algunas ocasiones los ataques serán mediante técnicas de ingeniería social[1] o ataques de denegación de servicio[2].
- **Amenazas externas accidentales.** En muchas ocasiones las amenazas son involuntarias o resultantes de desastres naturales, que pueden derivar en muchos casos en inundaciones o incendios.
- **Amenazas internas intencionadas.** Una de las amenazas que deben resolver nuestros departamentos de informática es el propio personal de la organización, como podría ser un empleado con acceso a los recursos de la organización que sabe que va a ser despedido.
- **Amenazas internas accidentales.** Comprenden las malas prácticas por parte de un empleado, sin tener una mala intención, por ejemplo insertar un USB infectado en un ordenador corporativo.

Debemos tener presente las amenazas a las que está expuesta la organización y la forma en la que podemos hacerles frente.

1. Las técnicas de ingeniería social son tácticas de persuasión utilizadas para obtener información o datos de naturaleza sensible, como claves o contraseñas. Estas técnicas suelen aprovecharse de la buena voluntad o de falta de precaución de la víctima.

2. Denegación de servicio o DoS se refiere a las técnicas que tienen por objeto dejar inoperativo a un servidor (web, de ficheros,...) sobrecargándolo de peticiones. De esta forma impiden que los usuarios legítimos puedan utilizar los servicios por prestados por él.

3. BUENAS PRÁCTICAS

Una vez conocidas las amenazas que pueden afectar a nuestros activos de información, debemos aplicar una serie de medidas de seguridad básicas **[2]**. Además de la aplicación de las medidas organizativas y de cumplimiento legal, los departamentos de TI aplicarán medidas para:

- la gestión de los activos;
- la seguridad de las operaciones;
- la gestión de incidentes y la recuperación ante desastres;
- control de accesos a sistemas y aplicaciones.

3.1 GESTIÓN DE LOS ACTIVOS

Estas medidas tienen por objetivo identificar los activos de la organización y definir las responsabilidades de protección sobre los mismos. Esto incluye desde la realización de un inventario, hasta la definición de los usos aceptables. Igualmente la gestión de activos incluye la clasificación de la información **[3]** y la gestión de soportes.

3.1.1 IDENTIFICACIÓN DE LOS ACTIVOS

La gestión de los activos de una organización es uno de los aspectos más complicados y a la vez más claves en un departamento de informática. Son muchos los activos que gestionamos en una empresa (ordenadores personales, teléfonos móviles corporativos, tabletas, portátiles, proyectores, servidores, aplicaciones software, monitores, periféricos, etc.). Por ello es necesario que realicemos y mantengamos actualizado un **inventario** en el que los activos se encuentren clasificados y gestionados de la manera correcta.

Para la gestión del ciclo de vida completo de los activos debemos incluir dentro del inventario:

- identificador interno del activo;
- características básicas;
- clasificación de seguridad, si aplica;
- responsable del activo;
- proveedor, garantía y datos de mantenimiento;
- ubicación física;
- fecha de destrucción cuando sea el caso.

3.1.2 CLASIFICACIÓN DE LA INFORMACIÓN

Atendiendo a la importancia de los distintos activos de información para la empresa se ha de llevar a cabo una **clasificación** que permita aplicar a la misma las medidas de seguridad oportunas. Para la clasificación se pueden considerar, además de su antigüedad y valor estratégico, las tres propiedades: confidencialidad, integridad y disponibilidad.

Lo más usual es clasificar la información teniendo en cuenta solamente una de estas tres dimensiones, la confidencialidad. Se clasifica la información en tres niveles: confidencial, de uso interno e información pública. Esta aproximación es la más aceptada pues uno de los riesgos más críticos para cualquier negocio es la fuga de información **[4]** que no es más que una pérdida de la confidencialidad de la misma.

Es importante identificar toda la información que se maneja, **incluido el software, sin importar el soporte o su formato.** Se ha de registrar su ubicación y la persona o equipo responsable y clasificarla según los criterios de seguridad que sean más adecuados, incluidas las necesidades de cumplimiento legal que sean aplicables, según la actividad de la empresa. Esta clasificación será esencial para aplicar las medidas de seguridad adaptadas a la criticidad de cada «clase» de información para el negocio.

Una vez clasificada, aplicaremos las medidas necesarias para su protección. Estas medidas, que se concretarán en distintas políticas, se dirigen a definir:

- ubicaciones y dispositivos permitidos para el almacenamiento y uso de la información según su criticidad;
- cifrado de información crítica en tránsito o en almacenamiento;
- control de acceso a la información almacenada y a los servicios y programas para su tratamiento; permisos por roles, contraseñas robustas, etc.;
- control de uso de dispositivos externos de almacenamiento y de móviles o tabletas;
- control del uso de almacenamiento y servicios en la nube;
- destrucción segura de la información una vez terminada su vida útil;
- copias de seguridad y planes de recuperación;
- según la actividad de la empresa, archivado seguro de la información que se deba conservar y de los registros de actividad como garantía del cumplimento legal o normativo que aplique.

3.1.3 GESTIÓN DE SOPORTES

La gestión de soportes persigue evitar que se revele, modifique, elimine o destruya de forma no autorizada la información almacenada en los mismos. Para ello el departamento de TI debe implantar procedimientos para la gestión de los soportes extraíbles, su eliminación y su protección frente a usos indebidos.

Debemos prestar especial atención los activos móviles usados en la organización. Estos dispositivos pueden almacenar información confidencial de la empresa y tienen una alta probabilidad de pérdida o de sufrir un robo.

Por ello deberán estar etiquetados e inventariados indicando como mínimo:

- tipo y marca del dispositivo;
- persona asignada al dispositivo;
- número de serie;
- dirección MAC;
- tipo de uso.

3.1.4 GESTIÓN DE LA CONFIGURACIÓN

Una vez identificados los activos importantes, debemos diseñar y mantener una **Base de Datos de Gestión de Configuración** (CMDB) que contenga los elementos de configuración necesarios e importantes para proporcionar un servicio (equipos de trabajo, servidores, software de trabajo, redes, documentación, etc.), y la relación existente entre ellos.

Esta es una tarea tremendamente útil e importante, a pesar de la su complejidad, con la que podremos llevar una organización y seguimiento de las actualizaciones de todos estos elementos.

Además de mantenerla actualizada, deberemos realizar auditorías, revisar los cambios, entradas y salidas de material, accesos, incidencias, etc. Existen herramientas específicas que nos ayudarán a llevar un buen mantenimiento de nuestra CMDB.

Esto nos permitirá establecer las medidas de seguridad a aplicar a cada uno de los activos si fuera necesario y conocer el ciclo de vida de cada uno de ellos, desde su adquisición/creación hasta su destrucción.

3.2 SEGURIDAD DE LAS OPERACIONES

La seguridad de las operaciones abarca las actividades encaminadas a asegurar el correcto funcionamiento del equipamiento donde se realiza el tratamiento de la información, desde su instalación y puesta en marcha, pasando por su actualización y protección ante software malicioso y la realización de copias para evitar la pérdida de datos, hasta la monitorización y el registro de las incidencias.

3.2.1 PROCEDIMIENTOS Y RESPONSABILIDADES

Es recomendable que todas las tareas técnicas que realicemos en la organización estén debidamente documentadas. Esto nos permitirá establecer un procedimiento de actuación sobre una determinada tarea, realizándola siempre bajo los mismos criterios.

Esto también permitirá que diferentes personas del departamento puedan realizar una misma tarea, garantizando la continuidad de la tarea ante variaciones de personal. Es importante reducir en la medida de lo posible la existencia de personal «imprescindible» en el departamento de informática.

Los procedimientos que elaboremos deben ser diseñados para ser compatibles con futuras y previsibles iniciativas de construcción de nuevos sistemas de información.

3.2.2 INSTALACIÓN DE SISTEMAS Y APLICACIONES

Garantizar que la instalación de los sistemas y aplicaciones se realizan conforme a los requisitos de seguridad de la organización es una de las funciones que se debe desempeñar desde el departamento de **informática.**

Además de la instalación segura de los sistemas y las aplicaciones, es conveniente establecer diferentes entornos aislados entre sí, prestando especial atención al entorno de producción; de esta forma dispondremos de un entorno para realizar pruebas y evitar así cualquier impacto en el entorno de producción.

Antes de que los nuevos sistemas y aplicaciones se propaguen al entorno de producción, debemos realizar revisiones para asegurarnos de que:

- cumplen con los requisitos de seguridad;
- han sido aplicados todos los parches y actualizaciones necesarios;
- se han establecido los acuerdos de nivel de servicio (SLA);
- se satisfacen los requisitos de rendimiento y capacidad.

Además de tener distintos entornos, debemos realizar procesos documentados en el que se indique de qué manera se ha de realizar la propagación de un entorno a otro.

En el caso de que en la organización se realice desarrollo de software, se deben diseñar e implantar entornos para asegurar el ciclo de desarrollo. Serían necesarios los siguientes entornos:

- desarrollo
- pruebas
- producción

Además es necesario establecer claramente las personas autorizadas a realizar dichas acciones, siendo restrictivos en lo que respecta al entorno de producción. Por ejemplo, un desarrollador no debe poder acceder a una máquina que esté en producción; esta tarea la debe realizar un administrador de sistemas.

3.2.3 ANÁLISIS DE LAS CAPACIDADES DE LOS SERVIDORES

Periódicamente debemos realizar un análisis de capacidad de los servidores y dispositivos que tenemos en nuestra organización. Para ello, muchos equipos disponen de funcionalidades básicas de monitorización, y en el mercado hay herramientas que permiten realizar un seguimiento adecuado.

Los recursos que se disponen en un servidor son limitados, por lo que además de monitorizarlos correctamente, es necesario realizar un análisis de recursos y necesidades futuras previendo de esta forma evitar que los equipos y sistemas se saturen, con consecuencias indeseadas.

3.2.4 ACTUALIZACIÓNES DE SEGURIDAD EN LAS APLICACIONES

Para garantizar la protección de los sistemas de información de la organización, es necesario realizar una correcta gestión de actualizaciones y parches de seguridad. Debemos realizarla desde un punto de vista preventivo, manteniendo los sistemas, aplicaciones y soluciones de seguridad en un nivel correcto de parcheado y actualización. De esta forma evitaremos que algún agujero (conocidos como vulnerabilidades o *bugs*) pueda afectar a nuestros sistemas.

Para mantener una gestión eficaz de actualizaciones de seguridad tenemos que:

- **Realizar revisiones** periódicas de los sitios web de proveedores de las aplicaciones y, en especial, de las notificaciones de seguridad, para identificar las nuevas actualizaciones de software y los nuevos problemas de seguridad que puedan afectar a nuestros sistemas informáticos.
- Determinar **en qué medida** afecta el fallo encontrado a la seguridad de nuestros sistemas.
- **Aplicar las actualizaciones** necesarias conforme a las instrucciones del fabricante.
- **Verificar** que el sistema está funcionando correctamente una vez aplicada la actualización.

Es recomendable que mantengamos un registro de todas las actualizaciones y parcheados, de esta forma nos será mucho más sencillo poder llevar un control y un seguimiento de los parches y actualizaciones que han sido instalados o faltan por instalar.

3.2.5 GESTIÓN Y CONTROL DE SISTEMAS ANTIVIRUS

Debemos verificar que todos los equipos se encuentren en el sistema de gestión del antivirus corporativo, y que se realicen correctamente los análisis periódicos de los equipos, para evitar infecciones.

Hoy en día existen multitud de herramientas **[1]** que nos facilitarán la ejecución de este trabajo, por lo que un mantenimiento adecuado, no resulta complicado. Debemos tener una buena gestión acompañado de una programación de revisiones periódicas para corroborar que todo se realiza correctamente.

3.2.6 COPIAS DE SEGURIDAD

Una de las medidas de seguridad más importantes es la **implantación de un sistema de copias de seguridad [3]** que nos garantice la recuperación de los datos y la continuidad del negocio en caso de que se materialice alguna amenaza que afecte a los mismos.

Debemos definir e implantar diferentes procesos para la gestión de las copias de seguridad, incluyendo **pruebas de restauración periódica** para garantizar que se realizan adecuadamente.

Además es importante adoptar medidas de seguridad adicionales para proteger las copias contra pérdida, daño o acceso no autorizado:

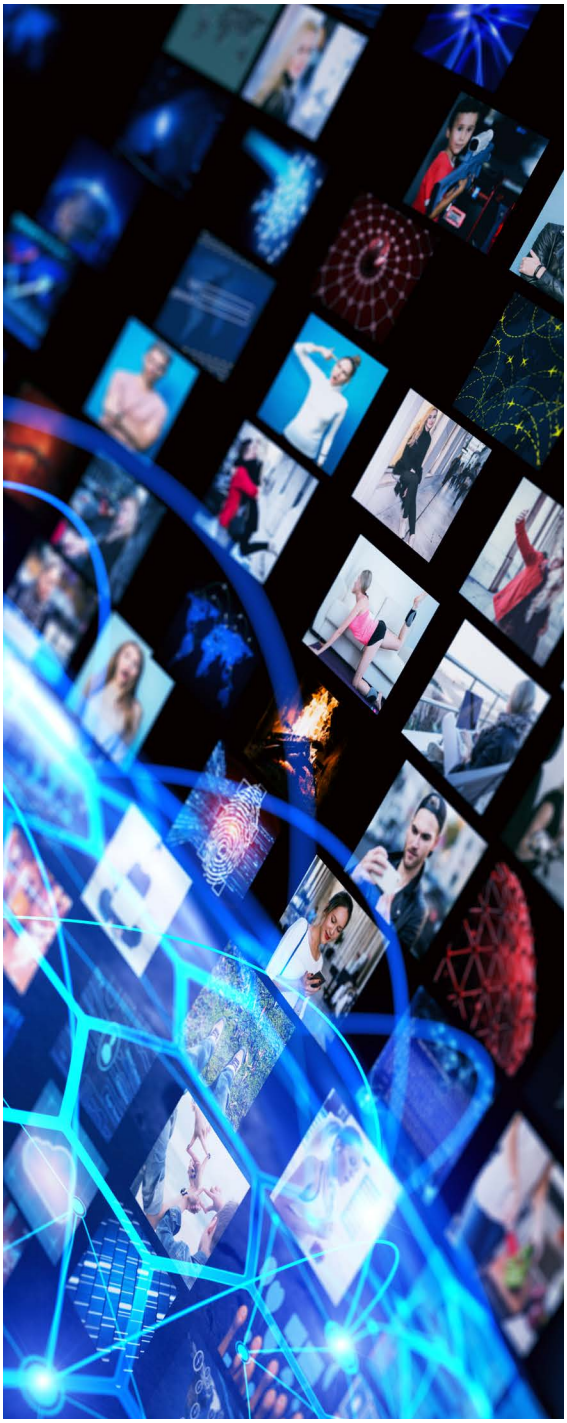
- Almacenar las copias en **medios físicos** (cintas, DVD, discos duros externos...). Para elegir convenientemente el método de almacenamiento, tenemos que basarnos en las especificaciones de los fabricantes: tasa de transferencia, capacidad y durabilidad del soporte.
- Almacenar las copias en **sitios cerrados seguros**, en una ubicación distinta del original para poder restaurar la información en caso de desastre.
- **Restringir el acceso a las ubicaciones** donde se encuentran las copias exclusivamente a las personas autorizadas.

También tenemos la opción, como alternativa al medio físico, de utilizar la **nube** (servicios de copias de seguridad online) como lugar de almacenamiento o replicación de las copias de seguridad de la organización.

3.2.7 GESTIÓN DE LA MONITORIZACIÓN

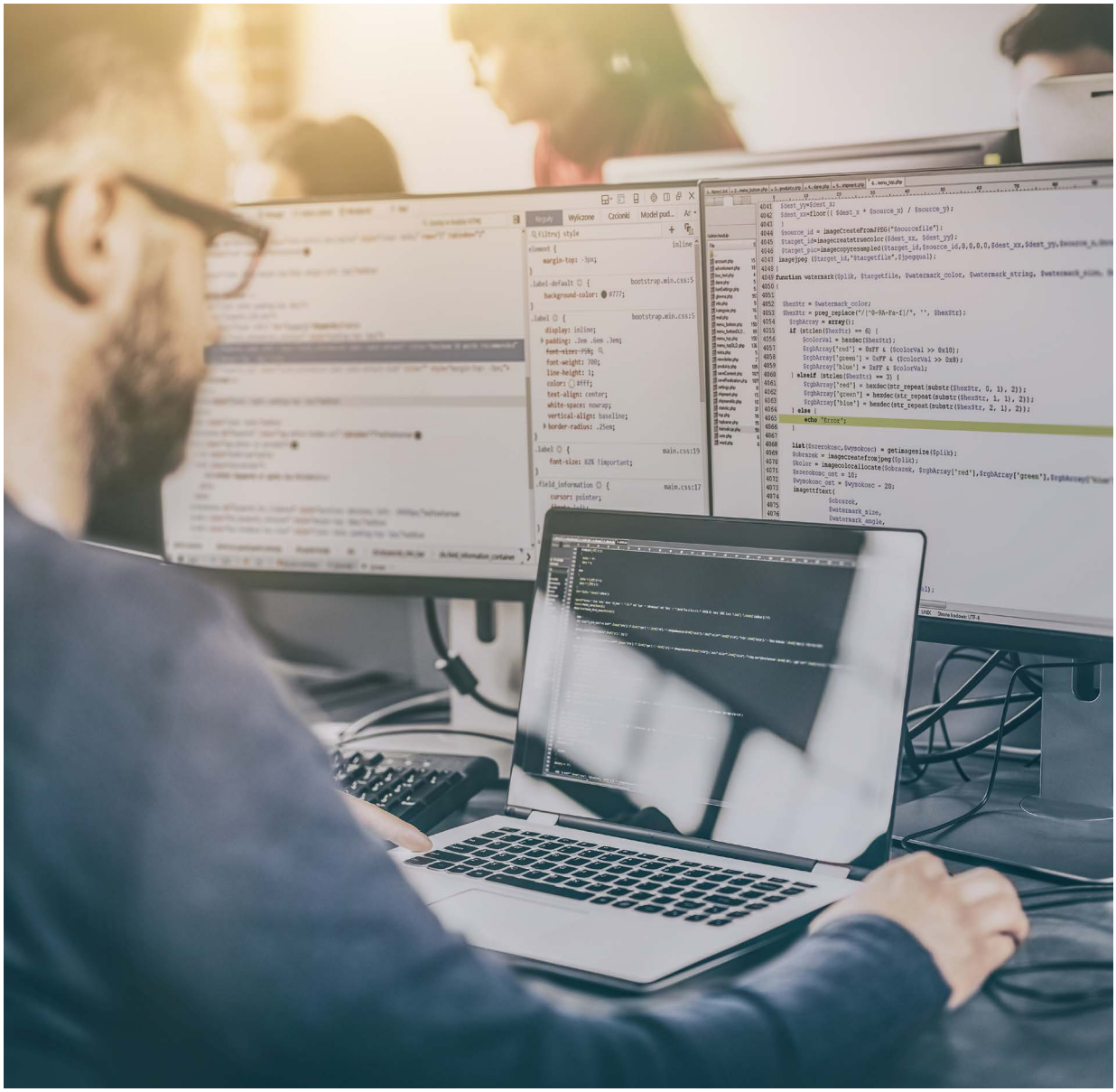
Es imprescindible en cualquier empresa tener un sistema que controle diferentes parámetros de los sistemas tecnológicos tales como la carga de un SAI, la temperatura de los CPD, los registros de los sistemas antivirus, los elementos de seguridad de la red, el volumen de tráfico de la salida a Internet o la propia carga de CPU o Disco Duro de cualquier servidor.

Es conveniente que este tipo de aplicativos tengan sistemas de aviso ante cortes, pérdidas de servicio o fallas puntuales, y que además permitan obtener informes periódicos de cada elemento para tener un registro y poder prever de manera proactiva cambios o sustituciones que pueden evitar fallos posteriores.



3.3 GESTIÓN DE INCIDENTES Y RECUPERACIÓN ANTE DESASTRES

Para estar preparados en caso de un incidente de seguridad o de resultar afectados por un desastre natural es necesario conocer cómo debemos gestionarlos. En ambos casos se han de establecer previamente las responsabilidades y los procedimientos de actuación como medida preventiva para saber cómo actuar en caso de que ocurran.



3.3.1 GESTIÓN DE INCIDENCIAS DE SEGURIDAD

Los incidentes de seguridad son eventos de diferente naturaleza y a menudo con consecuencias negativas: fallos en los sistemas, acceso no autorizado a datos sensibles, ataques de denegación de servicio, etc.

En general, podemos considerar un **evento de seguridad** como un incidente que afecta o trata de afectar a la integridad, confidencialidad o disponibilidad de la información o los sistemas que la gestionan y almacenan. **[4] [5]**

El departamento de informática tiene la responsabilidad de gestionar dichos incidentes pero, para hacerlo de una manera eficiente, debemos abordar una serie de actividades conjuntas para tal fin:

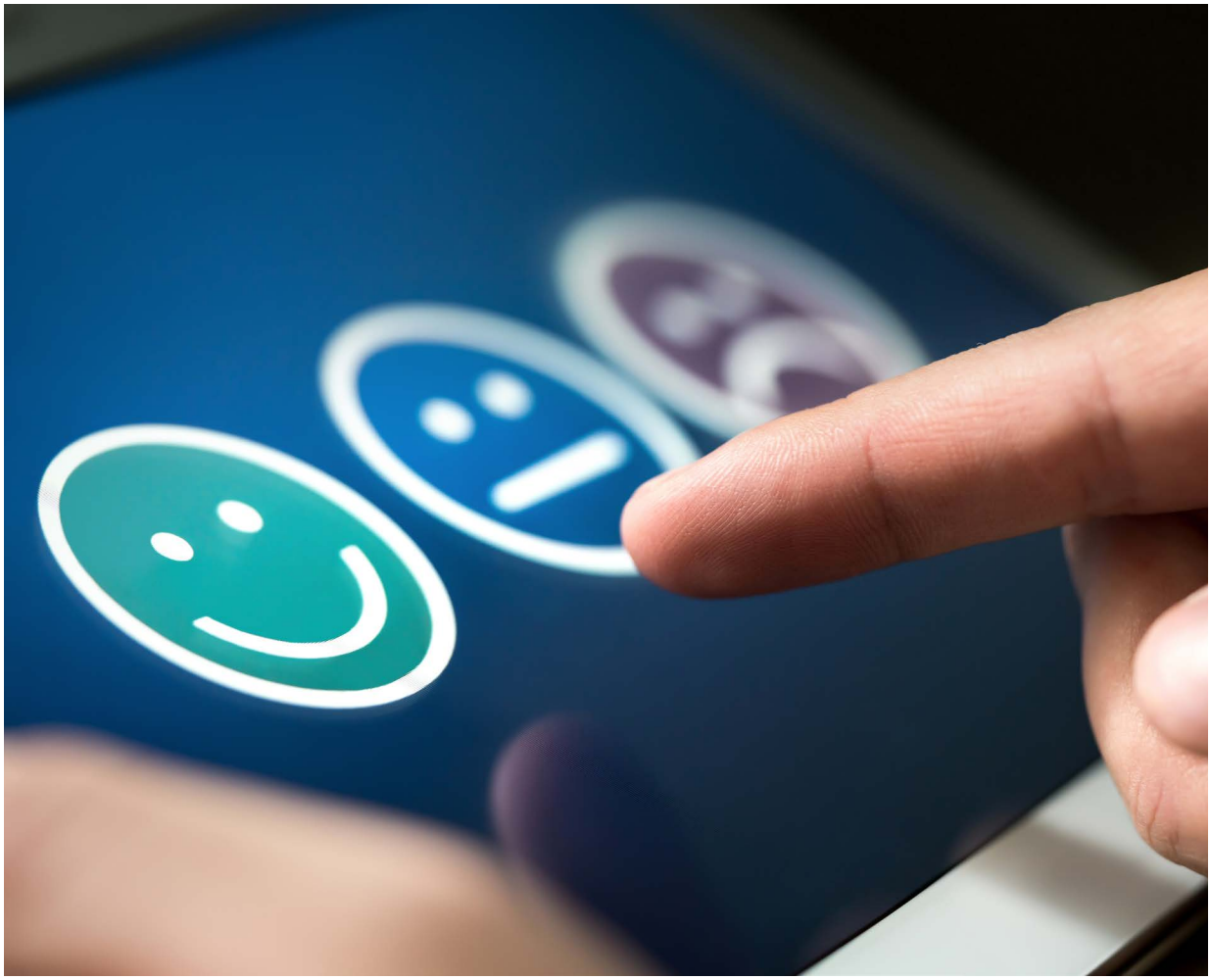
- Debemos establecer **sistemas de recolección de eventos** que nos permita poder monitorizar las alertas de seguridad.
- **Analizar los incidentes de seguridad** detectados, documentarlos y catalogarlos determinando su prioridad.
- **Estudiar los incidentes** que se hayan producido, analizar sus causas, y establecer medidas adicionales que protejan a los activos de nuevos incidentes de similar naturaleza.
- Poner en marcha un **punto central de comunicación**, tanto para recibir como para difundir información de incidentes de seguridad a las partes correspondientes sobre el evento.
- Establecer **procedimientos de respuesta** ante incidentes y mantenerlos actualizado para saber qué pasos debemos de dar para una correcta gestión.

3.3.2 PLAN DE RECUPERACIÓN ANTE DESASTRES

El **plan de recuperación ante desastres** (DRP o *Disaster Recovery Plan* por sus siglas en inglés) es un plan que cubre la restauración de los datos, el hardware y el software crítico de la organización ante un desastre. De este modo el negocio podría continuar con sus servicios y operaciones ante cualquier incidente.

Para llevar a cabo el plan de recuperación ante desastres, debemos conocer los riesgos a los que estamos expuestos y que pueden perjudicar la operación habitual del negocio.

Para más detalle se puede consultar el bloque temático Plan de contingencia y continuidad de negocio **[5]**.



3.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Para prevenir el acceso no autorizado a los sistemas y aplicaciones se debe restringir el acceso a los mismos de acuerdo a una política definida por la organización. Esta política limitará el acceso a los recursos, evitando accesos no autorizados y garantizando el acceso de los usuarios autorizados. Estas políticas abarcan el control del acceso físico y lógico.

El control del acceso físico evitará la pérdida, daño, robo o alteración de los activos y la interrupción de las operaciones. Algunas de estas medidas son la separación de áreas, los tornos de acceso, etc.

En cuanto al acceso lógico se han de implantar, cuando sean necesarios, procedimientos de acceso seguro de inicio de sesión (autenticación[3]), y sistemas interactivos para establecer y cambiar con frecuencia las contraseñas de forma que sean seguras y robustas.

3. Procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

3.4.1 CONTROL DE ACCESO A APLICACIONES CRÍTICAS Y ZONAS RESTRINGIDAS

En toda organización existen zonas y aplicaciones consideradas críticas, a las que no debe tener acceso todo el personal, ya que en ellas se almacenan información confidencial o de suma importancia.

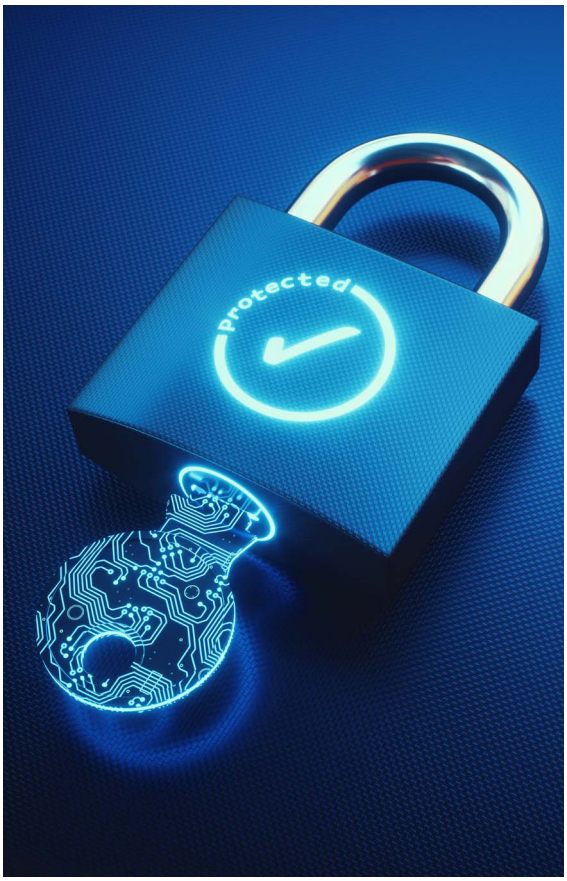
Debemos implementar una política de control de accesos sobre los activos críticos de la organización, para minimizar el riesgo de posibles fugas de información.

Para ello es importante:

- **Inventariar y catalogar** las aplicaciones y las zonas de la organización en base a su criticidad, estableciendo de esta forma cuáles son susceptibles de aplicar unas restricciones u otras.
- **Establecer los criterios de acceso** basándonos exclusivamente en la necesidad funcional. Es decir, debemos aplicar un criterio de acceso conocido como *need-to-know*: no todos los miembros de la organización requieren acceso a toda la información de la misma. Es decir, una persona debe tener acceso a las aplicaciones críticas o zona restringida solo cuando el ejercicio de su trabajo lo requiera.

Además de establecer la política de control de accesos, es importante que se almacenen los **registros de los accesos realizados**. De esta forma tendremos trazabilidad si se producen accesos no deseados a aplicaciones o a zonas restringidas. Debemos **revisar los accesos periódicamente** para verificar que son accesos autorizados.

Como medida adicional, es interesante que limitemos el tiempo de conexión en las aplicaciones consideradas como críticas. Así evitaremos que por despiste de un empleado al abandonar su puesto dejándose una aplicación abierta, personal no autorizado pueda acceder a la información.



3.4.1.1 CONTROL DE ACCESOS LÓGICOS

El control de accesos lógico está formado por los mecanismos para hacer cumplir los criterios que se establezcan para permitir, restringir, monitorizar y proteger el acceso a nuestros servicios, sistemas, redes e información. Para ello tenemos que identificar a los usuarios, quienes son y qué les vamos a permitir hacer.

En primer lugar es necesario dar de alta en los sistemas a los usuarios y gestionar de forma automática todo el ciclo de vida de sus identidades.

Para identificar a los usuarios se utilizan:

- credenciales como el ID de usuario y la contraseña;
- permisos, derechos y privilegios;
- atributos, como el horario o el cargo para nuestros empleados;
- información biométrica, etc.

Después se ha de comprobar que los usuarios que intentan acceder son realmente quienes dicen ser (autenticación). Para la autenticación se pueden utilizar distintos factores y en ocasiones más de uno a la vez: contraseñas, PIN, OTP (*One Time Password*), *passphrases, smartcards*, claves criptográficas o biometría en sus distintas formas.

Una vez ya sabemos quién quiere acceder a qué hemos de verificar si cumple los atributos (tiene el cargo adecuado y está dentro del horario o en la ubicación prevista, por ejemplo) y tiene los permisos y privilegios para autorizarle o no.

Por último el sistema tiene que registrar todo lo que ocurre en relación con los accesos, en la jerga en inglés: *accountability*. Registrar la actividad es esencial para poder realizar auditorías, comprobar que las políticas de acceso están bien implementadas y detectar intrusiones o actividades sospechosas. Los sistemas operativos y las aplicaciones disponen de esta funcionalidad pero es necesario activarla, configurarla y supervisar los resultados.

A modo de resumen:

- **Identificación** es el método mediante el cual decimos quienes somos, es decir, que nombre nos han puesto en el sistema, como nos reconoce. Así la identidad que accede mostrará su nombre de usuario o una id de proceso si es una máquina, por ejemplo.
- **Autenticación** es el método para comprobar que somos quienes decimos que somos. Esto se realiza generalmente con algo que poseemos, somos o sabemos y que previamente (al darnos de alta) el sistema había asociado a nuestra identidad. Es la segunda parte de las credenciales de acceso. Son ejemplos: contraseñas, claves criptográficas, PIN, huellas dactilares, etc.
- **Autorización** es el mecanismo para comprobar si el usuario autenticado tiene los derechos de acceso a los recursos que quiere acceder y los privilegios para hacer con ellos lo que solicita. Si es así, le autoriza, en caso contrario no.
- ***Accountability*** es el mecanismo para registrar todos los eventos que tiene lugar en relación con los accesos, básicamente: quién quiere acceder, a qué, cuándo, para qué y qué resultado tiene ese evento (accede, no accede, el recurso no está disponible, etc.).

Para un buen control de accesos se ha de establecer una **política de acceso** que defina una gestión de usuarios y una segregación de funciones. De esta política se derivan los procedimientos para la gestión de contraseñas (cada cuanto se deben cambiar, su fortaleza,...), para la gestión de alta/baja de usuarios (cuando entra un nuevo empleado por ejemplo o cuando abandonan la empresa) y sus permisos (perfiles por departamento o por funciones por ejemplo).

3.4.2 GESTIÓN DE USUARIOS Y SEGREGACIÓN DE FUNCIONES

La gestión de usuarios en una organización es una de las tareas que requiere que se realice de una manera meticulosa y organizada, ya que determinará el acceso que tendrá un usuario a la información corporativa. Por ello es importante al dar de alta a los usuarios de una organización, establecer quién puede acceder a cada tipo de información. En este punto puede ser útil realizar una matriz entre información y áreas o departamentos, si la organización lo permite.

La asignación de permisos sobre los recursos que contienen la información puede realizarse bien individualmente, bien por perfiles o grupos de usuarios.

Además, debemos tener presente que muchas veces no se cursa correctamente la baja de un usuario en los sistemas o queda algún usuario que no se tenía en cuenta en algún momento. No está de más programar informes que nos adviertan de usuarios inactivos en el sistema y poder así eliminar o deshabilitar aquellas cuentas de acceso al servidor que no sean necesarias.

Por ejemplo, podemos generar avisos mensuales de usuarios inactivos durante más de un mes. Así, con ésta información, podemos valorar la necesidad de cursar la baja de los mismos, evitando tener cuentas en el sistema de usuarios inactivos de cualquier tipo, ya sean cuentas de usuario, de VPN[4] o de algún aplicativo concreto.

4. Una red privada virtual, también conocida por las siglas VPN, del inglés *Virtual Private Network* es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet. Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autenticación y el cifrado.

La segregación de funciones evita que una misma persona lleve a cabo todas las actividades de un mismo proceso. Esto es especialmente importante en el ámbito de los departamentos de informática, por su acceso privilegiado a la mayor parte de los sistemas corporativos, y especialmente por la necesidad de que existan múltiples personas que puedan atender una incidencia.

Es conveniente que evitemos que una misma persona concentre el conocimiento y ejecución de las funciones críticas del departamento de informática. De lo contrario, corremos el riesgo de que se produzca una concentración de conocimientos o sobrecarga que pueden llevar a una mala ejecución de la función.

Por ejemplo, si únicamente una persona sabe recuperar las copias de seguridad, podríamos tener problemas para recuperar la información ante unas vacaciones o una baja de esa persona. Esto aplica también a caídas de servidores, actualizaciones, configuraciones del correo electrónico, etc. Además debemos contemplar la posibilidad de que un empleado abandone la empresa y posteriormente nos demos cuenta de que únicamente él sabía realizar ciertas tareas críticas.

Por ello, es conveniente que establezcamos una serie de políticas de respaldo para las actividades o funciones críticas de nuestro departamento de informática.

3.4.3 GESTIÓN SEGURA DE LAS CONTRASEÑAS

Es importante que realicemos una correcta gestión de las contraseñas que usamos para acceder a los distintos servicios de la organización, especialmente cuando se trate de usuarios de administración de los equipos. Debemos establecer una política segura en la creación, mantenimiento y cambio de contraseñas, con el fin de mantener la seguridad y la privacidad de la información.

Debemos seguir una serie de hábitos adecuados para la gestión de las claves:

- Que sean robustas, es decir, que tengan más de ocho caracteres y aparezcan mayúsculas, minúsculas, símbolos especiales (*/-+&%$) y números.
- Evitar contraseñas fáciles como nombres, palabras o expresiones que coincida con el propio usuario, que estén en blanco o que coincida con contraseñas anteriores que han sido utilizadas por el usuario.
- Las contraseñas han de caducar al menos cada 12 meses.
- Utilizar un gestor de claves para almacenarlas y realizar copias de seguridad regulares. Esto nos permitirá poder utilizar contraseñas robustas sin necesidad de memorizarlas.

4. REFERENCIAS

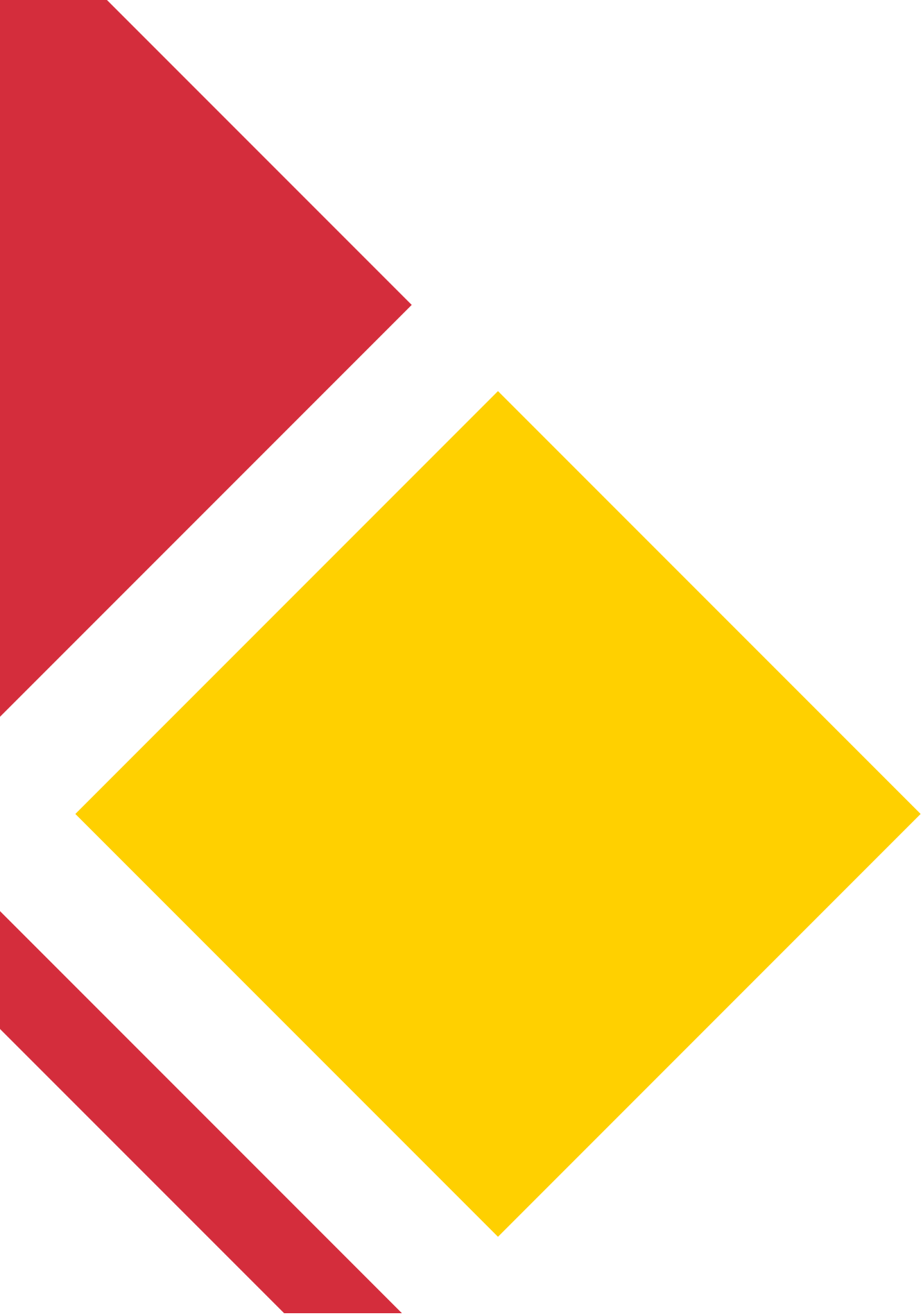
[Ref - 1]. INCIBE, Catálogo de empresas y soluciones de seguridad de INCIBE - https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

[Ref - 2]. INCIBE, Checklist de buenas prácticas de los departamentos de TI - https://www.incibe.es/sites/default/files/contenidos/dosieres/buenas-practicas-area-informatica/checklist-buenas-practicas.pdf

[Ref - 3]. INCIBE, Guía de almacenamiento seguro de la información. Una guía de aproximación al empresario - https://www.incibe.es/protege-tu-empresa/guias/almacenamiento-seguro-informacion-guia-aproximacion-el-empresario

[Ref - 4]. INCIBE, Cómo gestionar una fuga de información. Una guía de aproximación al empresario - https://www.incibe.es/protege-tu-empresa/guias/guia-fuga-informacion

[Ref - 5]. INCIBE, Plan de Contingencia y Continuidad de Negocio - https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio



GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa