CitNOW

Política sobre seguridad informática y de los datos

Última actualización:
17 de septiembre de 2017

www.**citnow**.com

Version en Español

Sistema/s comercial/es de CitNOW: todos
Referencia: ISO/IEC 27001 y 27002

Índice

Anexo

1. Política sobre seguridad de la información

1.1 Visión general

La información es un recurso clave en nuestra organización. La información que almacenamos incluye: nombres, direcciones de correo electrónico, números de teléfono móvil y matrículas de vehículos de clientes; información eVHC de clientes; datos administrativos, personales y financieros; red informática y sistemas de bases de datos; y código informático y de programación. Cualquiera que sea la manera en la que se recopila, accede o utiliza la información, nos aseguraremos de que esté protegida por las medidas de seguridad apropiadas, permitiéndonos lograr nuestras metas comerciales conforme a la legislación aplicable y cumplir nuestras obligaciones contractuales.

1.2 Objetivo

Nuestro objetivo de seguridad consiste en proteger nuestra organización frente a sistemas de seguridad como los siguientes: acceso no autorizado a los sistemas, violaciones de la confidencialidad (personas que obtienen o divulgan información indebidamente), integridad (información alterada o validada por error, tanto de manera deliberada como accidental) y disponibilidad (información que no está disponible cuando se necesita) o cualquier otra cuestión que podría afectar negativamente nuestra actividad comercial o la actividad comercial de nuestros clientes y proveedores.

1.3 Alcance

Esta política cubre todos los ordenadores, servidores y software que gestionamos.

1.4 Política

1.4.1 Enfoque

Nos comprometemos a:

Poner en práctica todas las medidas razonables, adecuadas, prácticas y efectivas para proteger nuestros procesos y activos a fin de lograr nuestro objetivo de seguridad.

Utilizar un Sistema de gestión de la seguridad de la información (SGSI) de conformidad con el estándar ISO/IEC 27001 como marco de trabajo que guíe nuestro enfoque hacia la gestión de la seguridad.

Revisar continuamente nuestro uso de las medidas de seguridad, de modo que podamos mejorar la manera en la que protegemos nuestro negocio.

Proteger y gestionar nuestros activos de información para permitirnos cumplir nuestras responsabilidades contractuales, legislativas y de privacidad.

1.4.2 Responsabilidades

Todos los empleados, tanto anteriores como actuales, fijos y eventuales, actuarán en todo momento de manera responsable, profesional y consciente de la seguridad manteniendo la conciencia y conformidad con esta política.

Todos los empleados respetarán los activos de información de terceros, tanto si dicha protección se requiere o no de manera contractual o legal.

Se exige a todos los empleados con responsabilidad de supervisión que promuevan activamente las mejores prácticas entre su personal supervisado.

Nuestro director general de Seguridad de la Información (CISO), que está directamente subordinado a nuestro CEO, es responsable de garantizar que la información en nuestra organización esté protegida de una manera adecuada, además de asegurar el logro de nuestro objetivo de seguridad. El CISO y el Panel de seguridad están autorizados por el CEO para adoptar las actuaciones y medidas adecuadas que contribuyan al logro de nuestro objetivo comercial y que sean acordes con esta Política sobre seguridad de la información.

Cada cierto tiempo, el CISO podría delegar determinadas acciones a individuos responsables y es responsable de asignar recursos suficientes de manera que podamos lograr nuestro objetivo de seguridad.

1.4.3 Prácticas

Identificaremos nuestros riesgos de seguridad y sus prioridades relacionadas respondiendo inmediatamente e implementando dispositivos de seguridad que sean adecuados, efectivos y prácticos.

Toda la información (incluida la información de terceros y la información personal) estará protegida por controles de seguridad y procedimientos de tramitación adecuados a su grado de sensibilidad e importancia.

Cuando estemos autorizados para ello, la información se hará disponible fuera de nuestra organización a terceros. Los propietarios de información serán responsables de identificar a quién se divulgará su información y deberán mantener registros completos y precisos de dicha divulgación.

Garantizaremos que nuestras actividades puedan continuar con una disrupción mínima u otros efectos negativos en caso de que sufra cualquier forma de disrupción o incidencia de seguridad.

Las incidencias de seguridad actuales o presuntas se notificarán inmediatamente al Panel de seguridad, el cual gestionará la incidencia y organizará un análisis de la incidencia y las lecciones consiguientes que hay que aprender. Las incidencias de seguridad relacionadas con los datos personales deberán gestionarse de conformidad con la ley sobre privacidad aplicable.

Esta política estará respaldada por procedimientos documentados y estándares, junto con educación y formación.

El cumplimento con la política será objeto de un seguimiento periódico por parte del Panel de seguridad, que se reunirá regularmente.

Nuestro CISO facilitará una revisión anual de esta política realizada por el Panel de seguridad, cuyo grado de integridad, efectividad y usabilidad se revisará. La efectividad se medirá a través de nuestra capacidad de evitar incidencias de seguridad y de minimizar los impactos resultantes.

Nuestro CISO aprobará todas las versiones nuevas de la Política sobre seguridad de la información. Todos nuestros empleados son responsables de identificar maneras en las que la Política sobre seguridad de la información podría mejorarse.

Las sugerencias de mejora deberán enviarse al Panel de seguridad. Si se requieren cambios inmediatos, se celebrará una reunión especial del Panel de seguridad; de otro modo, las sugerencias se analizarán en la reunión para llevar a cabo la revisión anual de la política.

1.4.4 Concienciación sobre la política

Una copia de esta política se pondrá a disposición de todos los empleados actuales o cuando se unan a nuestra organización. Las secciones individuales de la política se actualizarán como se requiera y estarán disponibles en nuestro sitio de intranet, Podio. Se espera que todos nuestros empleados estén familiarizados y cumplan con la Política sobre seguridad de la información en todo momento. Los miembros del Panel de seguridad serán responsables en primera instancia de la interpretación y aclaración de la Política sobre seguridad de la información. Los empleados que requieran más información acerca de cualquier aspecto de esta política deberán exponer sus necesidades a un miembro del Panel de seguridad.

1.4.5 Aplicabilidad y cumplimiento

Esta política se aplica a todos nuestros empleados y a aquellas personas que hacen uso de sus instalaciones y de la información. El cumplimiento de la política formará parte del contrato de empleo y todos los empleados serán responsables de sus acciones relacionadas con la seguridad de la información.

El incumplimiento de la Política sobre seguridad de la información podría perjudicar nuestra capacidad de alcanzar nuestras metas y objetivos de seguridad, y podría dañar el prestigio profesional de la organización. Como última penalización, el incumplimiento será tratado como una cuestión disciplinaria. Nuestro CISO será responsable de tomar todas las decisiones relacionadas con el cumplimiento de esta política empleando los procedimientos disciplinarios a su disposición según proceda.

Alentaremos la adopción y el uso de esta Política sobre seguridad de la información por parte de terceros que cooperen en empresas conjuntas.

2. Política sobre seguridad del servidor

2.1 Visión general

Los servidores no protegidos y vulnerables continúan siendo una vía de entrada principal para agentes de amenazas maliciosas. Las políticas coherentes de instalación de servidores, la propiedad y la gestión de la configuración giran en torno a llevar a cabo los principios básicos.

2.2 Objetivo

El objetivo de esta política consiste en fijar estándares para la configuración básica del equipo de servidores interno propiedad y/o explotado por nuestra organización. La implementación eficaz de esta política minimizará el acceso no autorizado a nuestra información y tecnología de propiedad.

2.3 Alcance

Todos los empleados, contratistas, consultores, trabajadores fijos y otros trabajadores en nuestra organización y nuestras filiales deben adherirse a esta política. Esta política se aplica al equipo de servidores propiedad, explotado o arrendado por nosotros o registrado bajo un dominio de red interna de nuestra propiedad.

2.4 Política

2.4.1 Requisitos generales

Todos los servidores implementados en nuestra organización deben ser propiedad de un grupo operativo responsable de la administración del sistema. Todos los servidores que traten con datos de clientes deben ser propiedad del grupo de desarrollo y operación del software (DevOps). Cada grupo operativo debe establecer y mantener los manuales aprobados de configuración del servidor en base a las necesidades comerciales y bajo la aprobación del Panel de seguridad. Los grupos operativos deberán supervisar el cumplimiento de la configuración e implementar una política de excepción especialmente adaptada a su entorno. Cada grupo operativo debe establecer un proceso para cambiar los manuales de configuración, que incluya la revisión y aprobación del Panel de seguridad. Deben cumplirse los requisitos siguientes:

- Todos los servidores deben estar registrados con DevOps. Como mínimo, es necesaria la información siguiente para identificar definitivamente el punto de contacto:
- Contacto(s) y ubicación del servidor, y un contacto de backup
- Los equipos informáticos y el sistema/versión operative
- Las funciones y aplicaciones principales, si procede
- La información proporcionada a DevOps debe mantenerse actualizada

- Los cambios en la configuración para los servidores de producción deben seguir los procedimientos de gestión de cambios adecuados

Por motivos de seguridad, cumplimiento y mantenimiento, el personal autorizado deberá supervisar y auditar el equipo, los sistemas, los procesos y el tráfico de red.

2.4.2 Requisitos de configuración

La configuración del sistema operativo debería hacerse conforme a las directrices aprobadas del Panel de seguridad.

Los servicios y las aplicaciones que no se utilicen deberán deshabilitarse cuando sea práctico.

De ser posible, el acceso a los servicios debería estar registrado y/o protegido mediante métodos de control de acceso, como un cortafuegos de aplicaciones web.

Los parches de seguridad más recientes deben instalarse en el sistema en cuanto sea factible, siendo la única excepción cuando la aplicación inmediata pudiera interferir con los requisitos comerciales.

Las relaciones de confianza entre los sistemas constituyen un riesgo de seguridad y su uso debería evitarse. No utilice una relación de confianza cuando cualquier otro método de comunicación sea suficiente.

Sírvase siempre de emplear principios de seguridad estándar del menor acceso requerido para realizar una función. No use ROOT cuando bastará con una cuenta sin privilegios.

Si se dispone de una metodología para una conexión de canal seguro (es decir, técnicamente viable), deberá llevarse a cabo el acceso privilegiado en los canales seguros (por ej., conexiones de red cifrada utilizando SSH o IPSec).

Los servidores deberán tener una ubicación física en un entorno de acceso controlado.

Se prohíbe específicamente que los servidores operen dentro de nuestras instalaciones de oficinas.

2.4.3 Supervisión

Todos los eventos relacionados con la seguridad en sistemas de importancia vital o confidenciales deben registrarse y los registros de auditoría deben guardarse como se indica a continuación:

- Todos los registros relacionados con la seguridad se mantendrán en línea en el servidor durante una semana como mínimo.
- Después, se configurarán los registros para transferirse al servidor de registros global para su archivo y almacenamiento.

Los eventos relacionados con la seguridad se notificarán al Panel de seguridad, el cual revisará los registros y las incidencias. Se prescribirán medidas correctivas cuando sea necesario. Los eventos relacionados con la seguridad incluyen entre otros:

- Ataques de exploración de puertos
- Evidencia de acceso no autorizado a cuentas privilegiadas
- Casos anómalos que no están relacionados con aplicaciones específicas en el host

2.5 Cumplimiento de la política

2.5.1 Medición del cumplimiento

El Panel de seguridad verificará el cumplimiento de conformidad con esta política a través de varios métodos, entre otros, rondas periódicas, informes de herramientas comerciales, auditorías internas y externas, y comentarios al propietario de la política.

2.5.2 Excepciones

Toda excepción a la política debe ser aprobada por el Panel de seguridad por adelantado.

2.5.3 Incumplimiento

Si se encuentra que un empleado ha infringido esta política, podría estar sujeto a una acción disciplinaria incluyendo la posible terminación de empleo.

3. Política sobre control y eliminación de activos informáticos

3.1 Visión general

Todos los empleados y el personal que tenga acceso a los sistemas informáticos de la organización deberán adherirse a la Política sobre control y eliminación de activos informáticos definida a continuación a fin de proteger la seguridad de la red, proteger la integridad de los datos y proteger y controlar los sistemas informáticos y los activos de la organización. La política sobre control de activos no solo permite que se realice un seguimiento de los activos de la organización en torno a su ubicación y quién los está utilizando, sino que también protege cualquier dato almacenado en dichos activos. Esta política sobre activos también cubre la eliminación de activos.

Los activos informáticos no deberían confundirse ni rastrearse con otros activos de la organización, como el mobiliario. Uno de los motivos principales para realizar un seguimiento de los activos informáticos, aparte de para el control y rastreo de la propiedad, es por motivos de seguridad informática. Una política especial de rastreo de activos informáticos permitirá a la organización adoptar medidas para proteger los datos y recursos de red.

Esta política definirá qué es lo que debe hacerse cuando se traslada parte de la propiedad de un edificio a otro o de una ubicación a otra. Esta política proporcionará una base de datos de rastreo de activos que debe actualizarse, de manera que se conozca la ubicación de todo el equipo informático.

Esta política ayudará a los administradores de red a proteger la red, ya que sabrán qué usuario y qué ordenador se encuentra en cuál estación en caso de que un gusano infecte la red. Asimismo, esta política cubre la posibilidad de que los datos en un ordenador que se trasladen entre instalaciones de seguridad podrían ser confidenciales y deben cifrarse durante el traslado.

3.2 Objetivo y responsabilidad

Esta política ha sido diseñada para proteger los recursos de la organización en la red estableciendo una política y un procedimiento para el control de activos. Dichas políticas ayudarán a prevenir la pérdida de datos o de activos de la organización y reducirán el riesgo de pérdida de datos debido a una planificación deficiente.

El director tecnológico (CTO) es el último responsable del desarrollo, la implementación y el cumplimiento de esta política.

3.3 Activos rastreados

En esta sección se define a qué activos informáticos debería hacérseles un seguimiento y en qué medida.

3.4 Tipos de activos informáticos

En esta sección se categorizan los tipos de activos sujetos a rastreo:

1. Terminales de estaciones de trabajo
2. Ordenadores portátiles
3. Teléfonos móviles y tabletas
4. Impresoras, copiadoras, faxes, máquinas multifunción
5. Dispositivos portátiles
6. Escáneres
7. Servidores
8. Cortafuegos
9. Routers
10. Conmutadores
11. Dispositivos de memoria

3.4.1 Activos rastreados

Los activos con un coste inferior a £100 GBP no se rastrearán específicamente, incluidos componentes informáticos como tarjetas de vídeo o sonido. No obstante, deberán rastrearse los activos que almacenen datos independientemente de cuál sea su coste. Entre estos activos se incluyen:

1. Discos duros
2. Unidades de almacenamiento temporal
3. Cintas con datos almacenados, incluyendo datos de backup del Sistema

4. Aunque no se rastreen específicamente, esta política cubre otros dispositivos de almacenamiento, como discos de CD ROM y discos flexibles, con fines de eliminación y almacenamiento seguro

3.4.2 Dispositivos de memoria pequeños

Los activos de almacenamiento de memoria pequeños no se rastrearán por ubicación, sino por administrador. Entre estos activos se incluyen:

1. Discos flexibles
2. Discos de CD ROM
3. Memorias extraíbles

Si se permite el uso de este tipo de dispositivos para algunos empleados, el administrador del dispositivo debe firmar el recibo de dichos dispositivos en su posesión. Asimismo, todos los empleados deben aceptar el tratamiento responsable de memorias extraíbles, discos flexibles y discos de CD ROM, así como el seguimiento de las siguientes directrices:

1. Nunca colocar datos confidenciales en ellos sin autorización. Si se colocan datos confidenciales en ellos, deberá obtenerse un permiso especial y el dispositivo de memoria deberá mantenerse en un área segura.
2. Nunca colocar datos de cliente en ellos.
3. Nunca utilizar estos dispositivos para introducir programas ejecutables de fuera de la red sin autorización y sin primero explorar el programa con un detector aprobado y actualizado antivirus y de malware. Deberá informarse de antemano al departamento informático de cualquier programa que se introduzca en la red para obtener autorización.

Consultar la Política sobre dispositivos extraíbles para obtener más información.

3.5 Requisitos de rastreo de activos

1. Todos los activos deben contar con un número de identificación; se asignará un número interno de rastreo cuando se adquiera el activo o cuando el uso de números de identificación del fabricante deba especificarse en esta política.
2. Se creará una base de datos para el rastreo de activos en la que se incluirá toda la información en la tabla de la Lista de comprobación para la cesión de activos y la fecha del cambio del activo.
3. Cuando se adquiera un activo, se asignará un número de identificación para el activo y se introducirá su información en la base de datos para el rastreo de activos.

3.6 Procedimiento de cesión

3.6.1 Lista de comprobación para la cesión de activos

Cuando un tipo de activo enumerado en la lista de tipos de activos se transfiere a una ubicación o administrador nuevo, el administrador del ítem deberá cumplimentar la Lista de comprobación para la cesión de activos informáticos y un representante autorizado de la organización deberá aprobarla. El administrador es la persona bajo el cuidado del elemento. Si el elemento es una estación de trabajo, el administrador será el usuario más habitual del puesto de trabajo. Para otro tipo de equipo, el administrador es el principal responsable del mantenimiento o la supervisión del equipo.

El administrador deberá cumplimentar el formulario con la Lista de comprobación para la cesión de activos e indicar si se trata de un activo nuevo, si se está trasladando a una ubicación nueva, si se está cediendo a un administrador nuevo o si se está eliminando. Deberá introducirse la información siguiente:

1. Tipo de activo
2. Número de identificación
3. Nombre del activo
4. Ubicación actual
5. Administrador designado
6. Ubicación nueva
7. Administrador nuevo
8. Ubicaciones de datos confidenciales

Una vez que el administrador cumplimente y firme el formulario con la Lista de comprobación para la cesión de activos, este deberá firmarlo un representante autorizado.

3.6.2 Introducción de datos

Una vez completado el formulario con la Lista de comprobación para la cesión de activos, se entregará al director de bases de datos para el rastreo de activos. Este garantizará que la información de los formularios se introduzca en la base de datos para el rastreo de activos en un plazo de una semana.

3.6.3 Comprobación de la base de datos

Los directores que gestionan proyectos que afectaron a la ubicación del equipo deberán comprobar periódicamente si los activos cedidos recientemente se añadieron a la base de datos. La base de datos deberá proporcionar una lista de cesiones recientes que pueda comprobarse con facilidad. Los directores deberán comprobar la base de datos cada semana para asegurarse de que los activos cedidos en las últimas dos o tres semanas estén incluidos en la base de datos.

3.7 Cesiones de activos

Esta política se aplica a cualquier cesión de activos, incluido lo siguiente:

1. Compra de activos
2. Reubicación de activos
3. Cambios de administrador del activo, incluyendo cuando un empleado deja la organización o es sustituido
4. Eliminación de activos, incluido:
5. Activo devuelto al fabricante o distribuidor debido a una devolución en garantía
6. Activo arrendado devuelto al arrendador

En todos estos casos, deberá cumplimentarse una Lista de comprobación para la cesión de activos.

3.8 Saneamiento de los dispositivos

Cuando se ceden activos a otro administrador, toda información confidencial en el dispositivo deberá protegerse y/o destruirse. El método de destrucción de datos depende de la confidencialidad de los datos en el dispositivo y del siguiente usuario del dispositivo (si se encuentra dentro de la organización y sus controles o fuera de la organización).

3.9 Eliminación de activos

La eliminación de activos es un caso especial, ya que todos los datos confidenciales en el activo deberán eliminarse durante o antes de la eliminación. El director del usuario del activo debe determinar el nivel de confidencialidad máximo de los datos almacenados en el dispositivo. A continuación, se enumera la medida a adoptar para el dispositivo en función del nivel de confidencialidad de los datos de conformidad con el proceso de evaluación de los datos:

1. Ninguna (No clasificada): sin obligación de borrar los datos aunque, en aras de prudencia, borrar normalmente los datos empleando cualquier medio como el saneamiento, la destrucción física o la desimantación.
2. Baja (Sensible): borra los datos empleando cualquier medio como el saneamiento electrónico, la destrucción física o la desimantación.
3. Media (Confidencial): los datos deben borrarse empleando una tecnología aprobada para garantizar que no puedan ser leídos con técnicas especiales de alta tecnología.
4. Alta (Secreta): los datos deben borrarse empleando una tecnología aprobada para garantizar que no puedan ser leídos con técnicas especiales de alta tecnología. Las tecnologías aprobadas se precisan en un documento de Procedimiento de eliminación de datos en dispositivos por tipo de activo, donde se incluyen los siguientes:

    1. Disco flexible
    2. Memoria extraíble
    3. Disco de CD ROM
    4. Cinta de almacenamiento
    5. Disco duro
    6. Memoria RAM

7. Memoria ROM o dispositivos de memoria ROM

3.10 Uso de los dispositivos

Esta política define los tipos de datos que podrían almacenarse en un dispositivo extraíble y si dicho dispositivo podría extraerse de una instalación físicamente segura y bajo qué condiciones podría permitirse. Entre los dispositivos extraíbles se incluyen:

1. Disco flexible
2. Disco de memoria
3. Disco de CD ROM
4. Cinta de almacenamiento

A continuación se enumera la política a adoptar para el dispositivo en función de la clasificación de confidencialidad de los datos almacenados en el dispositivo de conformidad con el proceso de evaluación de los datos:

1. No clasificada: los datos podrían extraerse con la aprobación de un superior y el permiso es permanente para la duración del empleo del empleado salvo que sea revocado. Podría enviarse el dispositivo a otras oficinas mediante cualquier transportista público o privado.
2. Sensible: los datos solo podrían extraerse de áreas seguras con el permiso de un director o un nivel superior de dirección y las aprobaciones solo se aplican a una única ocasión.
3. Confidencial: los datos solo podrían extraerse de áreas seguras con el permiso de un vicepresidente o un nivel superior de dirección. Deberán aplicarse ciertas precauciones de seguridad documentadas tanto para el método de transporte como en el destino.

4. Secreta: los datos solo podrían extraerse de áreas seguras con el permiso del presidente o un nivel superior de dirección. Deberán aplicarse ciertas precauciones de seguridad documentadas tanto para el método de transporte como en el destino.
5. Alto secreto: los datos nunca podrían extraerse de áreas seguras.

3.11 Dispositivos propiedad del empleado

La política define los tipos de dispositivos propiedad del empleado que los empleados pueden utilizar en las instalaciones de la empresa.

1. Los teléfonos móviles de propiedad personal pueden utilizarse en las instalaciones, pero no deberán conectarse a la red de la empresa a través de wifi.
2. No se permite el uso de ningún otro dispositivo propiedad del empleado en las instalaciones y no deben conectarse a la red de la empresa a través de cable o wifi.

3.12 Cumplimiento

Puesto que la seguridad e integridad de los datos, junto con la protección de recursos, tienen una importancia vital para el funcionamiento de la organización, los empleados que no se adhieran a esta política podrían estar sujetos a medidas disciplinarias incluyendo la posible terminación de empleo. Se exige a todo empleado que sea consciente de cualquier infracción de esta política que lo notifique a su supervisor u a otro representante autorizado.

3.13 Formación del empleado y reconocimiento de la política

Se espera que cada empleado en la organización sea consciente de las políticas y los procedimientos vigentes relacionados con la seguridad informática Cda empleado ecibirá formación sobre dichas políticas y procedimientos cada año como mínimo. Se exige a los empleados que firmen una confirmación donde se indique que son conscientes de la política y que cumplirán sus requisitos.

4. Política sobre dispositivos extraíbles

4.1 Visión general

Los dispositivos extraíbles son una fuente bien conocida de infecciones de malware y está directamente vinculada a la pérdida de información confidencial en muchas organizaciones.

4.2 Objetivo

El objetivo de esta política consiste en minimizar el riesgo de pérdida o exposición de la información confidencial que mantenemos y reducir el riesgo de adquirir infecciones de malware en ordenadores que utilizamos.

4.3 Alcance

Esta política cubre todos los ordenadores y servidores explotados en nuestra organización.

4.4 Política

Nuestros empleados solo pueden utilizar dispositivos extraíbles en sus ordenadores profesionales de nuestra propiedad. Nuestros dispositivos extraíbles no se pueden conectar ni utilizar en ordenadores que no sean propiedad nuestra o que arrendemos sin la autorización explícita de nuestro Panel de seguridad.

La información confidencial solo deberá almacenarse en dispositivos extraíbles cuando se exija para llevar a cabo sus obligaciones asignadas o cuando se proporcione información requerida por agencias estatales o federales. Nunca deberán almacenarse datos de clientes en dispositivos extraíbles.

Podrían solicitarse excepciones a esta política caso por caso y solo podrán aprobarse por parte del Panel de seguridad.

4.5 Cumplimiento de la política

4.5.1 Gestión del cumplimento

El Panel de seguridad verificará el cumplimiento de conformidad con esta política a través de varios métodos, entre otros, rondas periódicas, informes de herramientas comerciales, auditorías internas y externas, y comentarios al propietario de la política.

4.5.2 Excepciones

Toda excepción a la política debe ser aprobada por el Panel de seguridad por adelantado.

4.5.3 Incumplimiento

Si se encuentra que un empleado ha infringido esta política, podría estar sujeto a una acción disciplinaria incluyendo la posible terminación de empleo.

5. Política sobre virus y códigos maliciosos

5.1 Visión general

Esta política y procedimiento cubre nuestra Política sobre virus y códigos maliciosos.

5.2 Objetivo

El objetivo de esta política consiste en explicar el enfoque que debería adoptarse dentro de nuestra organización para evitar virus y códigos maliciosos, y qué hacer en caso de que ocurra una infección.

5.3 Alcance

Esta política cubre todos los ordenadores y servidores explotados en nuestra organización.

5.4 Política

Dado que los agresores están pasando de ataques que simplemente resultan molestos o destructivos a actividades motivadas por beneficios económicos, los ataques con códigos maliciosos se han vuelto más sofisticados y preocupan mucho a las organizaciones. Un ataque a gran escala con un código malicioso, que suele conocerse como un brote debido a un código malicioso, puede causar daños y trastornos generalizados a una organización, y requiere un periodo de recuperación más amplio y mayores esfuerzos. Por tanto, es crucial implementar medidas preventivas adecuadas, como la aplicación de herramientas de protección y detección, para salvaguardar una organización frente a ataques con códigos maliciosos.

No obstante, no existe nada parecido a una protección infalible en el mundo de la seguridad de la información. Además, es importante que la organización desarrolle un procedimiento sólido para incidencias relacionadas con la seguridad de la información, de manera que el personal esté mejor preparado para abordar brotes debidos a códigos maliciosos de una manera más organizada, eficiente y efectiva.

Todo proceso de respuesta a una incidencia debería contar con tres etapas principales: «Planificación y preparación», «Respuesta» y «Evaluación de los daños». Esta sección muestra los pasos en las etapas de «Respuesta» y «Evaluación de los daños» que son importantes para abordar plenamente brotes debidos a códigos maliciosos. Si desea obtener más información acerca de la etapa de «Planificación y preparación», consulte la sección de la política «Tratamiento de incidencias de seguridad para empresas».

La etapa de «Respuesta» consiste en los cinco pasos siguientes:

- Detección e identificación
- Escalada
- Contención
- Erradicación
- Recuperación

5.4.1 Detección e identificación

5.4.1.1 Determinar plenamente si ha ocurrido un brote debido a un código malicioso

El objetivo de este paso es determinar si ha ocurrido un brote debido a un código malicioso. Las indicaciones típicas de un brote debido a un código malicioso incluyen una o todas las situaciones siguientes:

- Los usuarios se quejan del acceso lento a Internet, agotamiento de recursos del sistema, acceso lento al disco o sistema de arranque lento.
- Se ha generado una serie de alertas por un sistema de detección de intrusos en un host (HIDS), por un antivirus o por un software de detección de un código malicioso.
- Se ha producido un aumento significativo del uso de la red.
- Se han constatado una serie de entradas de violaciones de acceso en registros de router de perímetro o en registros de cortafuegos.
- Se ha detectado un arranque de tráfico SMTP rebotado que surge de unas direcciones de IP internas.
- Se ha detectado un gran número de exploraciones de puertos e intentos fallidos de conexiones.
- El administrador del sistema nota una desviación inusual de los flujos de tráfico de red habituales.
- Los controles de seguridad, como el software de antivirus y cortafuegos personales, se han deshabilitado en muchos hosts.
- Inestabilidad y caídas del sistema general.

Tras el descubrimiento de alguno de los síntomas anteriores, el personal informático debería inmediatamente comprobar y validar todas las actividades sospechosas a fin de determinar si ha ocurrido un brote. Una vez que se haya confirmado que se trata de una infracción de seguridad debido a un código malicioso, es importante recabar información sobre el código malicioso, ya que esto será esencial para el proceso de contención y erradicación.

Puede obtenerse información acerca de códigos maliciosos en sitios web de proveedores de software de antivirus si el código malicioso ha estado circulando durante cierto tiempo, revisando las alertas del software de antivirus y de detección de códigos maliciosos y examinando archivos de registro del cortafuegos y del router. Las preguntas siguientes pueden ayudar a identificar las características del código malicioso:

- ¿Qué clase de código malicioso es (un gusano de red, un gusano de envío masivo por correo electrónico, un virus, un troyano, etc.)?
- ¿Cómo se propaga el código malicioso? (¿Atacando servicios de red vulnerables? ¿Por correo electrónico masivo?)
- Si el código malicioso se propaga atacando un servicio vulnerable, ¿cuál es la vulnerabilidad que se está explotando? ¿Se ha lanzado un parche para atajar la vulnerabilidad? ¿Cuáles son los servicios o puertos que están siendo atacados?
- ¿Pone el código malicioso puertas traseras en el sistema infectado?
- ¿Cómo se puede eliminar el código malicioso del sistema afectado? ¿Existe alguna herramienta de eliminación disponible?

5.4.1.2 Realizar evaluaciones preliminares

Una vez que se identifique una brecha, el equipo informático deberá evaluar el alcance, los daños y el impacto de la brecha a fin de tratar la cuestión con eficacia.

5.4.1.3 Registrar todas las medidas adoptadas

El equipo informático deberá registrar todas las medidas adoptadas para abordar la brecha y los resultados correspondientes. Esto puede facilitar la identificación y evaluación de la incidencia, y proporcionar pruebas para la acusación u otra información útil en etapas posteriores para el tratamiento de incidencias. Deberán realizarse registros durante el proceso completo de respuesta relacionado con la incidencia de seguridad

5.4.1.4 Contención

El tercer paso de respuesta a una incidencia debida a un código malicioso es la contención. A continuación, se enumeran actividades que deberían llevarse a cabo en la etapa de contención:

5.4.1.5 Identificar sistemas infectados

Identificar con claridad los sistemas infectados es siempre el primer paso de contención. Lamentablemente, también se trata de un proceso muy complicado debido a la naturaleza dinámica del entorno informático de hoy en día. Estas son algunas sugerencias que podrían ayudar a identificar sistemas infectados en un entorno gestionado.

- Llevar a cabo una exploración de virus exhaustiva en todos los sistemas con las últimas firmas de virus, además de con los motores actualizados de detección antivirus y de reparación. Ya que ningún software antivirus por sí solo ni herramienta de detección de códigos maliciosos puede destapar todos los tipos de códigos maliciosos, podría ser necesario utilizar más de una herramienta de exploración antivirus para garantizar que se hayan detectado todos los códigos maliciosos.
- Revisar todos los archivos de registro de routers y cortafuegos
- Proporcionar a los usuarios instrucciones sobre cómo identificar infecciones
- Configurar IPS o IDS para identificar actividades asociadas con infecciones
- Llevar a cabo rutinas de analizador de protocolos (sniffer) en busca del tráfico de red que coincida con las características del código malicioso

5.4.1.6 Contener el brote

Contener el brote puede hacerse de varias maneras; a continuación se indican tácticas habituales:

- Utilizando herramientas automatizadas
  La contención de la propagación de un código malicioso puede hacerse con herramientas automatizadas, como un software antivirus o herramientas de detección de códigos maliciosos, IDS e IPS. Si los sistemas de protección antivirus existentes no detectan el código malicioso, incluso si se aplica la última firma de virus, deberá buscarse la asistencia de proveedores de software antivirus para crear una firma nueva que cubra el código malicioso.

- Deshabilitando la conectividad
  na brecha debido a un código malicioso puede contenerse con efectividad desconectando rápidamente los sistemas infectados de la infraestructura de red general, algo que puede conseguirse aplicando controles de acceso a dispositivos de red o desconectando físicamente los cables de red. En algunos casos, a fin de contener la propagación de un código malicioso a otras secciones de la organización, podría ser necesario desconectar temporalmente los segmentos de la red afectados de la red central. No obstante, esta estrategia de contención afectará definitivamente al funcionamiento de otros sistemas no infectados en el segmento.
- Deshabilitando servicios
  El código malicioso podría propagarse a través de los servicios de red, por ejemplo, las unidades compartidas en la red. Bloquear temporalmente, incluso apagar los servicios de red utilizados por códigos maliciosos, ayuda a contener incidencias.
- Eliminando la vulnerabilidad
  El código malicioso podría propagarse atacando servicios de red vulnerables. Al tratar con las vulnerabilidades que han sido explotadas por el código malicioso, como la aplicación de parches de seguridad en sistemas vulnerables, pueden eliminarse los canales de propagación y, por tanto, contenerla. Además, el código malicioso también podría aprovechar algunos errores de configuración, como controles de acceso poco rígidos en unidades compartidas en red. La propagación de un código malicioso puede contenerse rectificando cualquier error de configuración.

- A través de la participación del usuario
  La participación del usuario es importante en el proceso de contención en un entorno en el que solo una cantidad limitada de personal de asistencia técnica está disponible para abordar un brote, por ejemplo, en sucursales pequeñas y remotas o en un entorno de oficina no gestionado. Deberá proporcionarse a los usuarios instrucciones claras sobre cómo identificar infecciones y qué medidas deberían adoptar si se confirma que un sistema está infectado como, por ejemplo, ejecutar las herramientas antivirus de eliminación.

5.4.1.7 Mantener registros de todas las medidas adoptadas

Es importante mantener un registro sólido de todas las acciones adoptadas en esta etapa, ya que algunas medidas de contención podrían requerir modificaciones temporales de la configuración o de los ajustes de la infraestructura de red y sistemas. Estas modificaciones deberán eliminarse tras la incidencia.

Es importante comprender que parar la propagación de la infección por un código malicioso no evita necesariamente que se produzca un daño futuro a sistemas infectados. Por ejemplo, la infección puede contenerse deshabilitando la conectividad a la red. Aún así, el código malicioso podría seguir borrando archivos activamente en el sistema infectado.

Por tanto, deberá llevarse a cabo un proceso de erradicación completo lo antes posible o simultáneamente con el proceso de contención.

5.4.2 Erradicación

Debe diseñarse la erradicación de un brote debido a un código malicioso para eliminar el código malicioso de todos los sistemas y dispositivos infectados, además de para rectificar la causa de la infección. Antes de llevar a cabo el proceso de erradicación, es aconsejable recabar toda la información necesaria, incluidos todos los archivos de registros, que podría ser necesaria borrar o restablecer durante el proceso de limpieza, algo que será útil en investigaciones posteriores.

El software antivirus o de exploración de códigos maliciosos y las herramientas de eliminación se utilizan habitualmente como medios principales de erradicación.

Sin embargo, en algunos casos podría ser necesario reconstruir los sistemas infectados desde cero. Por ejemplo, si el código malicioso se ha descargado y colocado una puerta trasera en los sistemas infectados, la medida más fiable a adoptar podría ser la reconstrucción de todos los sistemas a fin de restaurar la integridad de los sistemas. La reconstrucción de un sistema suele incluir las medidas siguientes:

- Reinstalar el sistema a partir de una fuente fiable, como un disco de instalación del sistema o una imagen de sistema fiable y limpio.
- Proteger sistemas de nueva instalación, por ejemplo, comprobando y garantizando que se hayan aplicado en cada equipo las últimas firmas de virus, además de los motores actualizados de detección antivirus y de reparación, y los parches de seguridad necesarios.
- Restaurar los datos a partir de dispositivos de backup conocidos y limpios.

5.4.3 Recuperación

Está claro que el objetivo principal del paso de recuperación consiste en restaurar el funcionamiento normal de todos los sistemas. En un brote debido a un código malicioso, es posible que ya se haya llevado a cabo la recuperación de la funcionalidad y de los datos de sistemas infectados como parte del proceso de erradicación. Aparte de restaurar los sistemas infectados, eliminar cualquier medida de contención temporal, como la suspensión de conexiones a la red, es otro aspecto principal del proceso de recuperación.

Antes de retirar las medidas de contención, un paso importante es realizar una evaluación de los riesgos para la seguridad anterior a la producción, a fin de garantizar que no se detecte ninguna infección y de que se rectifique la causa de la infección original.

Deberá notificarse a todas las partes relacionadas antes de la reanudación de los servicios suspendidos. El personal informático deberá restaurar las funciones específicas y los servidores etapa por etapa, de manera controlada y según el orden de demanda, por ejemplo, deberán reanudarse primero los servicios más esenciales o aquellos que asistan a la mayoría. Tras la reanudación de los servicios suspendidos, es importante verificar que la operación de restauración se haya realizado con éxito y que todos los servicios hayan vuelto a funcionar con normalidad. Podrían implementarse medidas de supervisión adicional para vigilar que no ocurra ninguna actividad sospechosa en los segmentos de red en cuestión.

5.4.4 Evaluación de los daños

Restaurar los sistemas infectados a su funcionamiento habitual no constituye el fin de un brote debido a un código malicioso. También es importante adoptar las medidas de seguimiento adecuadas. Estas incluyen la evaluación completa del daño causado, mejoras del sistema para evitar que se repita la incidencia, actualizaciones de políticas y procedimientos de seguridad y una investigación del caso para una posterior acción judicial. Entre las actividades que se incluyen en esta etapa están las siguientes:

- Revisar la efectividad de los procedimientos y mecanismos de protección existentes frente a virus/códigos maliciosos, incluido el control y la gestión centralizada de la distribución y detección de firmas de virus, y reparar las actualizaciones del motor, la exploración periódica programada en busca de virus, etc.
- Actualizar las políticas, las directrices y los procedimientos relevantes cuando sea necesario.
- Hacer cumplir las nuevas medidas de seguridad introducidas en la política/ directrices/procedimientos para proteger los sistemas frente a ataques futuros.
- Recordar a los usuarios que sigan las mejores prácticas en cuanto a seguridad, por ejemplo, no abrir mensajes de correo electrónico procedentes de fuentes electrónicas desconocidas/sospechosas, actualizar los parches de seguridad y las definiciones de virus periódicamente y cuando sea necesario, etc.

6. Procedimiento para la gestión de incidentes

6.1 Objetivo

El objetivo de esta política consiste en garantizar la rápida detección de eventos y deficiencias de seguridadasí como la rápida reacción y respuesta a las incidencias de seguridad.

6.2 Alcance y usuarios

Esta política se aplica al alcance del Sistema de gestión de seguridad de la información (SGSI) en su totalidad, es decir, a todos los empleados y a otros activos utilizados dentro del alcance del SGSI, además de a los proveedores y a otras personas fuera de la organización que entran en contacto con los sistemas y la información dentro del alcance del SGSI.

Los usuarios de esta política son todos nuestros empleados, además de todas las personas anteriormente mencionadas.

6.3 Referencia

- Estándar ISO/IEC 27001, cláusulas A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6 y A.16.1.7
- Estándar ISO/IEC 27001, cláusulas 16.1.1, 16.1.2, 16.1.7 y 18.1.2

6.4 Política

Una incidencia de seguridad de la información es un «evento único o una serie de eventos de seguridad de la información no deseados o imprevistos que tienen una probabilidad importante de comprometer las operaciones comerciales y de amenazar la seguridad de la información».(ISO/IEC 27000:2009).

6.4.1 Política

Una incidencia de seguridad de la información es un «evento único o una serie de eventos de seguridad de la información no deseados o imprevistos que tienen una probabilidad importante de comprometer las operaciones comerciales y de amenazar la seguridad de la información».(ISO/IEC 27000:2009).

6.4.2 Procedimiento de tratamiento para deficiencias o eventos de seguridad

La persona que recibió la información sobre una deficiencia o evento de seguridad analiza la información, establece la causa y, si fuera necesario, sugiere medidas preventivas y correctivas.

En situaciones en las que están involucrados los servicios online o la información personal de identificación del cliente, el director de seguridad debe decidir si los clientes, con quienes se relaciona la deficiencia o el evento de seguridad, deben ser informados (si no fue el cliente quien emitió el informe inicial). Siempre que los clientes deban ser informados, las notificaciones deberán hacerse lo antes posible, por teléfono o en persona, siguiendo los procedimientos acordados.

6.4.3 Tratamiento de incidencias de menor importancia

Si se notificó una incidencia de menor importancia, la persona que recibió la información, junto con el equipo del cliente y cuando sea necesario o se exija, debe adoptar los pasos siguientes:

1. Tomar medidas para contener la incidencia
2. Analizar la causa de la incidencia
3. Adoptar medidas correctivas para eliminar la causa de la incidencia
4. Informar a las personas involucradas en la incidencia, además de al director de seguridad, acerca del proceso de tratamiento de la incidencia

La persona que recibió la información acerca de una incidencia de menor importancia debe registrar la incidencia con el director de seguridad a través del correo electrónico y plantear un defecto en Jira para poner al equipo de desarrollo sobre aviso.

6.4.4 Tratamiento de incidencias de mayor importancia

En el caso de que produjeran incidencias de mayor importancia que pudieran causar algún tipo de disrupción durante un periodo de tiempo inaceptable, se llevará a cabo uno de los procedimientos siguientes:

Durante el horario laboral:

1. Se celebra una reunión de urgencia del Panel de seguridad
2. Se evalúan la gravedad y la seguridad de la incidencia
3. Se toma una decisión acerca de la mejor medida a seguir
4. Se adopta la medida
5. En cuanto sea posible, se lleva a cabo un análisis de la incidencia y lo revisa el Panel

Fuera del horario laboral:

1. La primera persona en ser notificada de la incidencia recaba los recursos técnicos que pueda encontrar
2. Se evalúan la gravedad y la seguridad de la incidencia y, si tratar de solucionarla fuera del horario laboral podría causar más daños si los recursos correctos no están disponibles
3. Se toma una decisión acerca de la mejor medida a seguir
4. Se adopta la medida mínima
5. Durante el horario laboral se lleva a cabo una evaluación más exhaustiva con acciones adicionales si fuera necesario
6. En cuanto sea posible, se lleva a cabo un análisis de la incidencia y lo revisa el Panel

6.4.5 Aprendiendo de las incidencias

El Panel de seguridad debe revisar todas las incidencias de menor importancia cada tres meses y registrar las que se repitan, o aquellos eventos que podrían convertirse en incidencias de mayor importancia en la siguiente ocasión, en el Registro de incidencias.

El Panel de seguridad debe analizar cada incidencia registrada en el Registro de incidencias (tipo de identificación, grado de afinidad y coste de la incidencia) y, si fuera necesario, sugerir una medida preventiva o correctiva.

6.4.6 Medidas disciplinarias

El director de seguridad debe acogerse a un proceso disciplinario para cada infracción de las normas de seguridad junto con el departamento de RR. HH.

6.4.7 Recogida de pruebas

El Panel de seguridad definirá las normas sobre cómo identificar, recabar y preservar pruebas que serán aceptadas como evidencia en actuaciones legales y otras.

En situaciones en las que esté involucrada la información personal de identificación del cliente, el director de seguridad definirá, junto con el cliente de servicios en la nube, el procedimiento para identificar, recabar y preservar pruebas que serán aceptadas como evidencia en actuaciones legales y otras.

6.5 Gestionar los registros mantenidos en base a este documento

Nombre del registro	Ubicación de almacenamiento	Persona responsable del almacenamiento	Controles para la protección del registro	Tiempo de retención
Registro de incidencias	DropBox de la empresa	Panel de seguridad	Solo los miembros del Panel tienen derecho a editar el registro	Cinco años
Normas para identificar, recabar y preservar pruebas	DropBox de la empresa	Director de seguridad	Solo el director de Seguridad tiene derecho a editar y publicar las normas	Los registros se almacenan durante un periodo de cinco años

Solo el director de seguridad puede conceder acceso a otros empleados a los registros.

6.6 Validez y gestión del documento

Este documento es válido a fecha 5 de octubre de 2017.

El propietario de este documento es el director de seguridad, que debe comprobar y, si procede, actualizar el documento al menos una vez cada seis meses.

A la hora de evaluar la efectividad y la idoneidad de este documento, se deben considerar los criterios siguientes:

- El número de deficiencias o incidencias que no fue notificado a las personas autorizadas
- El número de incidencias que no fue tratado de la manera más adecuada
- El número de incidencias que no fue registrado en el Registro de incidencias
- El número de incidencias para el cual las pruebas para tomar acciones legales fueron inadecuadas
- El número de infracciones de las normas de seguridad donde no se invocó un proceso disciplinario

Las versiones anteriores de este procedimiento deben almacenarse durante un periodo de cinco años, salvo que se especifique de otra manera mediante requisitos legales o contractuales.

7. Política sobre copias de seguridad

7.1 Objetivo

El objetivo de este documento consiste en garantizar que las copias de seguridad se creen en intervalos definidos y se comprueben con regularidad.

7.2 Alcance y usuarios

Este documento se aplica al alcance del Sistema de gestión de seguridad de la información (SGSI) en su totalidad, es decir, al conjunto de la tecnología de información y comunicación dentro del alcance.

Los usuarios de este documento son nuestros empleados.

7.3 Referencia

Estándar ISO/IEC 27001, cláusula A.12.3.1

7.4 Policy

7.4.1 Backup Procedure

Deben crearse copias de seguridad para todos los sistemas de software, datos y vídeos.

La creación de copias de seguridad es un proceso automatizado y forma parte de los sistemas de software escritos y aplicados por nosotros. El director de DevOps es el último responsable de garantizar que las copias de seguridad se realicen y almacenen con éxito.

Se crean automáticamente registros del proceso de backup en los sistemas donde se hace la copia de seguridad.

El software del sistema se almacena en una serie de depósitos y utiliza Git, haciendo posible volver a versiones anteriores como parte del Sistema.

Los datos se replican en bases de datos esclavas, en otros servidores y en otros centros de datos. Las copias de seguridad binarias se realizan cada hora y se almacenan en Amazon S3. Las copias de seguridad nocturnas se realizan a diario y se almacenan en Amazon S3.

Los vídeos se duplican en Amazon S3 tan pronto como se procesan. Estos permanecen en el servidor principal y en S3 cinco días como mínimo. Una vez borrados del servidor principal, se almacenan únicamente en S3, no obstante, S3 se configura para ofrecer un alto nivel de redundancia.

7.4.2 Comprobar las copias de seguridad

El depósito del sistema de software se comprueba a diario con desarrolladores que trabajan en él.

Las copias de seguridad de los datos se comprueban a diario, ya que dichas copias se restablecen en un servidor de pruebas que actúa como parte del proceso de implementación.

Las copias de seguridad de los vídeos se comprueban constantemente, ya que los vídeos se reproducen desde el sistema de backup tras el periodo inicial de cinco días, y una programación de anomalías destaca cualquier vídeo que no se haya copiado en el backup de S3.

7.4.3 Gestionar los registros mantenidos en base a esta política

El depósito del sistema de software se comprueba a diario con desarrolladores que trabajan en él.

Nombre del registro	Ubicación de almacenamiento	Persona responsable del almacenamiento	Controles para la protección del registro	Tiempo de retención
Registros del proceso de backup en formato electrónico	Sistema que ejecuta el procedimiento de backup	Director de DevOps	Los registros son solo de lectura; no pueden borrarse ni editarse	Los registros se almacenan durante un periodo de dos años

7.4.4 Validez y gestión del documento

Este documento es válido a fecha 5 de octubre de 2017.

El propietario de este documento es el CTO, que debe comprobar y, si procede, actualizar el documento al menos una vez al año.

A la hora de evaluar la efectividad y la idoneidad de este documento, es necesario considerar el criterio siguiente:

El número de pruebas de backup sin éxito

Las versiones anteriores de esta política deben almacenarse durante un periodo de cinco años, salvo que se especifique de otra manera mediante requisitos legales o contractuales.

Anexo

I. Datos del Panel de seguridad

El Panel de seguridad se compone de los cargos siguientes como mínimo:

- Consejero responsable del Desarrollo y la Seguridad (CTO)
- Director general de Seguridad de la Información (CISO)
- Arquitecto general de Software
- Director de DevOps
- Director de Desarrollo

El Panel debe reunirse mensualmente.

El Panel revisará todas las incidencias notificadas en el mes anterior, incluidos cualquier informe de una investigación post mortem de la incidencia, y recomendará cambios en el sistema, prácticas, procedimientos o políticas.

El Panel revisará las incidencias frente a una lista de clientes y, si cualquiera se viera afectado, se pondrá en contacto con el cliente en cuestión mediante el método acordado.

II. Registro de incidencias

Las incidencias se clasifican en los tipos siguientes:

- Información relacionada (relacionada directamente con la tecnología de información y comunicación)
- Información no relacionada (el resto de incidencias)

Información sobre incidencias:

El Registro de incidencias es un documento de Google.

N.º	Fecha de la incidencia	Descripción breve (nombre) de la incidencia	Persona responsable de abordar la incidencia	Descripción detallada (impactos, duración, sistemas/datos afectados por la incidencia, etc.)	Costes (en moneda local) directos e indirectos	Referencia al formulario de medidas correctivas
1						
2						
3						
4						