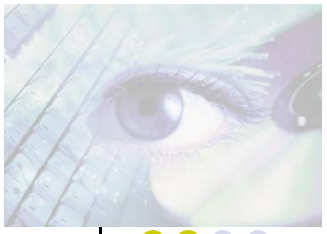
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, ISO 27001

Formación SGSI 2010

Centro Europeo de Empresas e Innovación Albacete



¿Qué es un Sistema de Gestión?

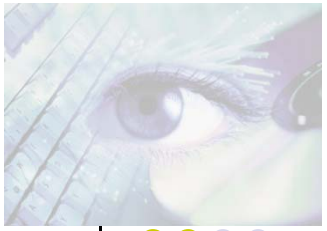
Un Sistema de Gestión implementa los procesos que permiten que una Organización realice un servicio o producto de manera confiable y en conformidad con unas especificaciones internacionales.

¿Qué aporta la ISO 27001 a la seguridad de la Información?

Aplica una arquitectura de gestión de la seguridad que identifica y evalúa los riesgos que afectan al negocio, con el objetivo de implantar contramedidas, procesos y procedimientos para su apropiado control y mejora continua.

Ayuda a la entidad a gestionar, de una forma eficaz, la seguridad de la información, **evitando las inversiones innecesarias, ineficientes o mal dirigidas** que se producen por contrarrestar amenazas sin una evaluación previa, por desestimar riesgos, por la falta de contramedidas, por implantar controles desproporcionados y de un coste más elevado del necesario, por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno, por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información, por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, etc.

Tengo un firewall, actualizo regularmente el antivirus y realizo copias de backup. ¿Qué aporta un SGSI a mi organización?



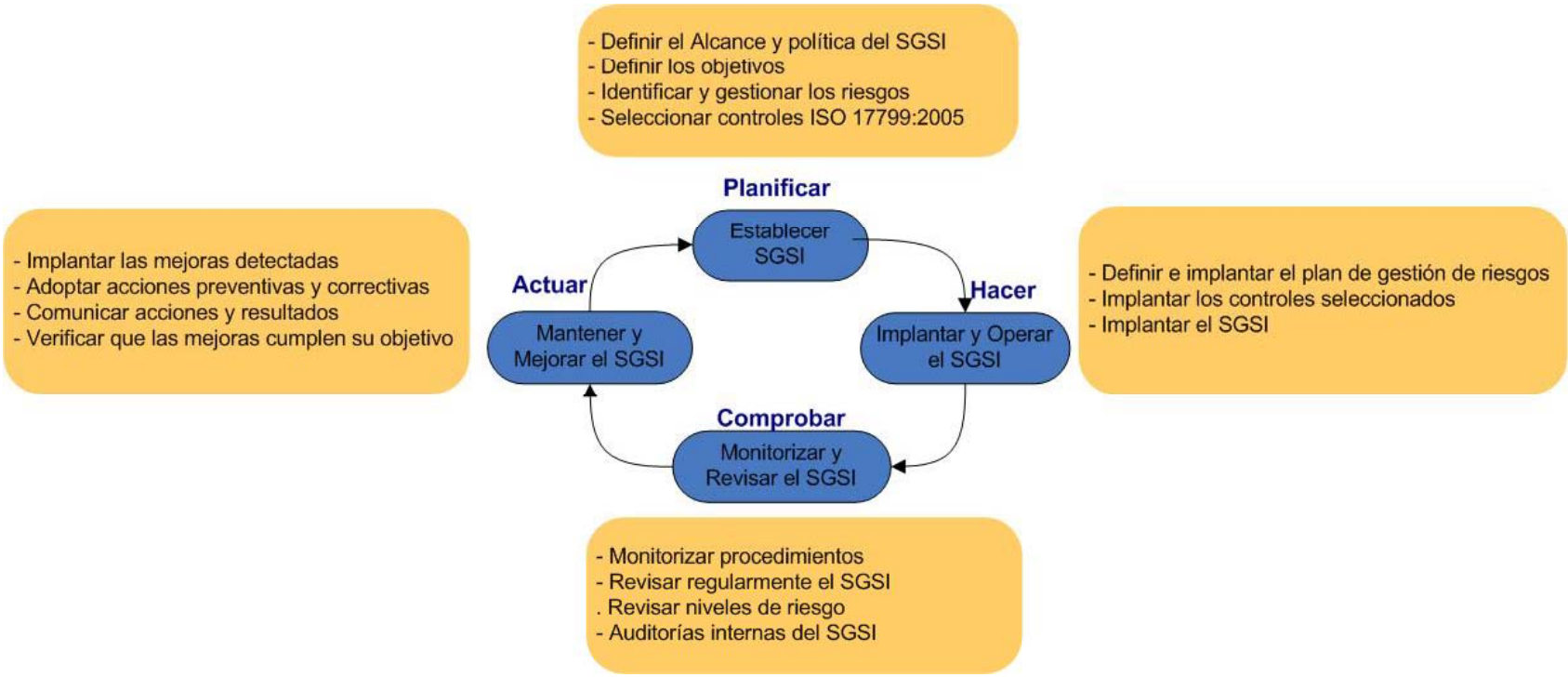
Estas medidas no son más que unos pocos controles técnicos que, por sí mismos, **NO SIGNIFICAN QUE SE ESTÉ GESTIONANDO LA SEGURIDAD**.

Un SGSI implica que la organización ha estudiado los riesgos a los que está sometida toda su información, ha evaluado qué nivel de riesgo asume, ha implantado controles (no sólo tecnológicos, sino también organizativos y legales) para aquellos riesgos que superan dicho nivel, ha documentado las políticas y procedimientos relacionados y ha entrado en un proceso continuo de revisión y mejora de todo el sistema.

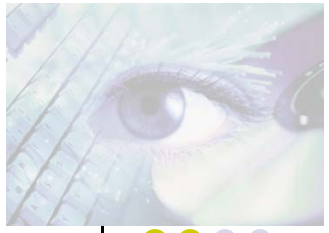
- **El SGSI da así la garantía a la empresa de que los riesgos que afectan a su información son conocidos y gestionados. No se debe olvidar, por tanto, que no hay seguridad total sino seguridad gestionada**.

¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.



Normas y estándares de Implantación de un SGSI



Para la implantación de un SGSI se consideran:

- **La norma ISO/IEC 27001:2005:** “Especificaciones para los Sistemas de Gestión de la Seguridad de la Información”, requeridas para obtener la certificación del SGSI implantado.

- **El estándar ISO/IEC 27002,** “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”. Estructurada en 11 dominios desglosados a su vez en 133 controles, que cubren todos los aspectos fundamentales de la seguridad en el tratamiento de la información.

¿Para qué sirve un SGSI?

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y actualiza constantemente.

¿Qué incluye un SGSI?

Un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles.

Documentos de Nivel 1

Alcance del SGSI
Política y objetivos de seguridad
Metodología de evaluación de riesgos
Informe de evaluación de riesgos
Plan de tratamiento del riesgo
Declaración de aplicabilidad
Procedimientos relativos al nivel 1

Fuente: www.ISO27000.es

ANÁLISIS DE RIESGOS

Proceso de identificar los riesgos de la seguridad, determinando su magnitud e identificando las áreas que requieren medidas de salvaguarda.

Implantación Tecnológica y Procedimental

1. Implantación Tecnológica:

Conectividad y Securización Integral de Redes de Información a través de:

- Implantación de cortafuegos
- Conectividad Securizada entre sedes
- Protección Antivirus
- Sistemas AntiSpam
- Soluciones de backups y copias de seguridad
- Planes de continuidad
- Protección de Contenidos
- Cumplimiento legislativo (LOPD, LSSICE)

Implantación Tecnológica y Procedimental

2. Implantación Procedimental:

Desarrollo y documentación de Procedimientos para:

- La Gestión de Incidencias
- Gestión Documental
- Gestión de Registros
- Control de Auditorías Internas
- Gestión de Recursos Informáticos
- Realizar Copias de Seguridad
- Planes de Recuperación y Continuidad
- …

Beneficios de Implantación de un SGSI

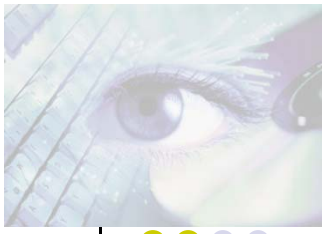
- Definir Objetivos y Metas
- Integrar la Gestión de la Seguridad de la Información con el resto de sistemas de gestión existentes de la entidad.
- Análisis de riesgos, identificando amenazas, vulnerabilidades e impactos, en su SGSI.
- Cumplimiento de la legislación vigente sobre protección de datos de carácter personal, comercio electrónico, etc.…(LOPD, LSSICE).
- Mejora continua de la gestión de la seguridad.
- Incremento de confianza de clientes y partners.
- Mejorar la imagen ante sus clientes, proveedores y empleados, convirtiéndose en un factor diferenciador frente a la competencia.
- Garantía de continuidad del negocio.

Beneficios de Implantación de un SGSI

Demuestra un compromiso unívoco de los órganos de Dirección de la Organización con el SGSI.

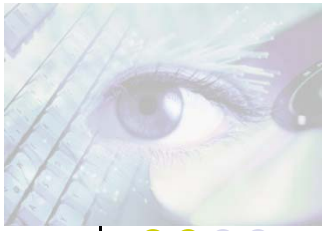
- **Aspecto Humano:** Mejora la sensibilización y responsabilidades del personal ante la seguridad en la organización.
- **Aspecto Financiero:** Reducción de los costos vinculados a los incidentes de seguridad.
- **Aspecto Organizacional:** El registro permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la organización en todos sus niveles.
- **Aspecto Funcional:** Gestión de los riesgos
- **Aspecto Legal:** Conformidad con leyes y normativas aplicables.
- **Aspecto Comercial:** Credibilidad y confianza de los socios, los accionistas y los clientes.

POLÍTICA DE SEGURIDAD



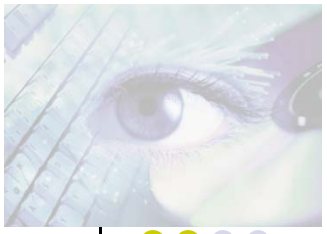
- Objetivos de Seguridad
  - **Garantizar la confidencialidad** de la información propia o proporcionada por nuestros clientes en relación a los servicios prestados.
  - **Garantizar la integridad, exactitud y veracidad de la información** generada o procesada en la realización de los servicios.
  - Asegurar que el acceso a los sistemas de información, relacionados con la prestación de los servicios, se realiza solamente por personal autorizado y con los privilegios de seguridad requeridos en relación al departamento o área a la que pertenece y según el desempeño de sus funciones.
  - Garantizar el cumplimiento de los acuerdos de nivel de servicio en relación a la seguridad de la información establecidos con terceros en la prestación de los servicios externos necesarios para la gestión de la Cámara.

POLÍTICAS DE SEGURIDAD



- USO ACEPTABLE DE LOS ACTIVOS
- USO CONTRA SOFTWARE MALICIOSO
- CONTROL DE ACCESOS
- USO DE CORREO ELECTRÓNICO
- PUESTOS DE TRABAJO DESPEJADOS
- USO DE CONTRASEÑAS DE USUARIO
- USO DE EQUIPOS PORTÁTILES

POLÍTICAS DE SEGURIDAD:
USO ACEPTABLE DE LOS ACTIVOS



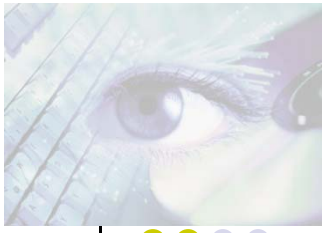
La información debe estar clasificada según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.

Se considera información a todo dato relacionado con las actividades y servicios de una organización, que tenga valor para ésta según estime su propietario, atendiendo a las escalas de valoración utilizadas, los requisitos legales, su sensibilidad y criticidad para la organización, cualquiera sea su forma y medio de comunicación y/o conservación (información de los sistemas, documentos impresos,…).

Toda información definida como activo debe ser clasificada para garantizar un nivel adecuado de protección.

Los soportes (CD, papel, Discos Duros,…) que contengan información de distintos niveles de clasificación serán clasificados con el nivel más alto de los activos de información que contengan.

POLÍTICAS DE SEGURIDAD:
USO ACEPTABLE DE LOS ACTIVOS



- **CLASIFICACIÓN DE LA INFORMACIÓN**

TRATAMIENTO DE LA INFORMACIÓN DE USO INTERNO:

Destrucción

-Soporte papel: Debe depositarse en papeleras dispuestas a tal efecto para posteriormente ser destruidos bajo control.
-Soporte electrónico: Antes de ser desechados o reutilizados, deben ser procesados para su borrado lógico o hacer ilegible la información contenida.

Etiquetado

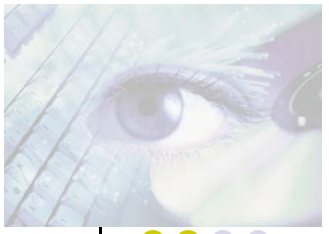
Toda información que disponga de la imagen corporativa de la entidad o sus formatos será automáticamente clasificada como de uso interno.

- Soporte papel: cualquier documento en formato corporativo se entenderá asignado al nivel de clasificación USO INTERNO.
- Soporte electrónico: Para los soportes propios o generados en la entidad, no será necesario el etiquetado del mismo salvo en los siguientes casos:

  Contengan datos de carácter personal de la entidad. En estos casos, deben aplicarse las medidas de seguridad definidas para el nivel medio en el R.D. 1720/2007 de desarrollo de la LOPD.

Centro Europeo de Empresas e Innovación Albacete

POLÍTICAS DE SEGURIDAD:
USO CONTRA SOFTWARE MALICIOSO



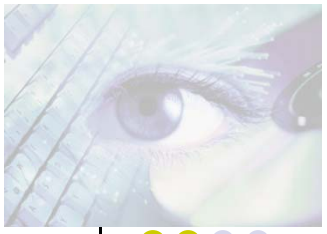
- No utilizar CD's, disquetes, memorias usb de fuera de las instalaciones en los equipos del sistema de información de la organización a menos que haya sido previamente verificado que están libres de virus u otros agentes dañinos.

- Los mensajes que se reciban de remitentes extraños o con contenido clasificable como *no relacionable con la actividad empresarial* deben ser eliminados en el acto, sin proceder a abrirlos.

- Estas acciones podrían suponer:

  - Posibles infecciones por instalación de software no fiable.
  - Violación de la Ley de Propiedad intelectual.
  - Daño de información contenida en los equipos, como pérdida o modificación irreversibles.

POLÍTICAS DE SEGURIDAD:
CONTROL DE ACCESOS A LA INFORMACIÓN



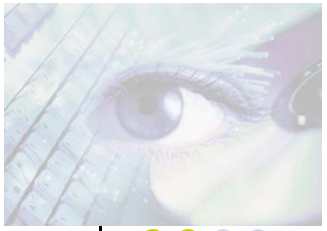
- Verificar que se activa el protector de pantalla de manera automática y que la reanudación del trabajo implica la desactivación de la pantalla protectora con la introducción de la contraseña de usuario correspondiente.

- Guarde documentos y dispositivos de almacenamiento (CDs, memorias, etc.) con información crítica o sensible en armarios o los cajones bajo llave.

- No deje documentos a la vista, por ejemplo:

  - Nombre de Usuario y Passwords
  - Direcciones IP
  - Contratos
  - Números de Cuenta
  - Listas de Clientes
  - Propiedad Intelectual
  - Datos de Empleados/ Currículums.

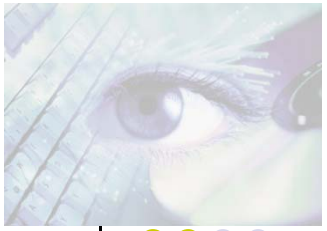
POLÍTICAS DE SEGURIDAD:
CONTROL DE ACCESOS A LA INFORMACIÓN



- El identificador de usuario tendrá unos privilegios asociados, en función del cargo y las funciones que desempeñe. Los privilegios asociados a cada usuario le permitirán, en función de cada caso, acceder a un determinado tipo de información.

- El uso de un identificador único hace posible el seguimiento de las actividades realizadas por los usuarios, otorgando así responsabilidad individual sobre las acciones.

POLÍTICAS DE SEGURIDAD:
SEGURIDAD FÍSICA Y DEL ENTORNO



Papeles y soportes informáticos.

- Guardarlos en cajones con llave y/o en archivadores.
- Destructora de Papel

Equipos personales y terminales

(impresoras, escáner, fotocopiadoras,..).

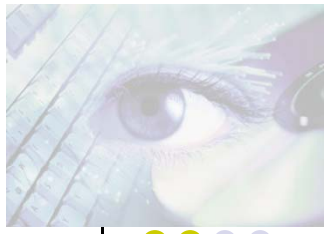
No dejar funciones y equipos de soporte desatendidos**, sobre todo si se va a imprimir o se está imprimiendo información confidencial de la empresa.**

- Protector de Pantalla con Contraseña

Las modificaciones de hardware y software serán realizadas EXCLUSIVAMENTE por el Departamento Técnico

ceei
Centro Europeo de Empresas e Innovación
Albacete

POLÍTICAS DE SEGURIDAD:
POLÍTICA DE CONTROL DE ACCESO



COMPROMISO DE CONFIDENCIALIDAD PARA EL PERSONAL

Todos los COMPROMISOS anteriores DEBEN MANTENERSE, incluso después de extinguida la relación laboral con organización.

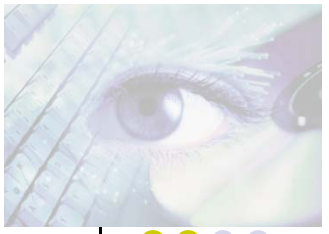
- **LOPD, LEY ORGÁNICA 15/1999 y R.D. 1720/2007**

▪ Obliga a las empresas que traten con datos de carácter personal a cumplir con una serie de obligaciones básicas.

▪ El incumplimiento de estas obligaciones está tipificado como infracción, con sanciones económicas entre **600 y 600.000 €.**

▪ Las especificaciones normativas pretenden establecer las **medidas técnicas y organizativas** idóneas para crear entornos empresariales que traten los datos personales de forma segura.

POLÍTICAS DE SEGURIDAD:
POLÍTICA DE USO DE CORREO ELECTRÓNICO



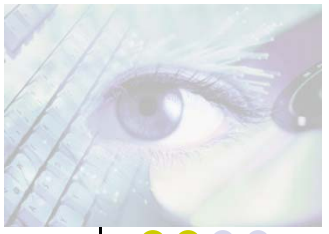
- Los usuarios que utilicen el correo electrónico dentro de la organización serán responsables de evitar prácticas que puedan comprometer la seguridad de la información.

- Los servicios de email corporativos se suministran para servir a propósitos operacionales y administrativos relacionados con el negocio. Todos los emails procesados por los Sistemas de Información corporativos y redes son considerados propiedad de la organización .

- **No usar el correo electrónico para:**

  - Para enviar información confidencial/sensible, particularmente a través de internet, a menos que ésta sea primero cifrada por un sistema de cifrado aprobado por el Dpto. Informático.
  - Para crear, enviar, reenviar o almacenar emails con mensajes o adjuntos que podrían ser ilegales o considerados ofensivos, p.e. sexualmente explícitos, racistas, difamatorios, abusivos, obscenos, discriminatorios u otros ofensivos.
  - Para enviar un mensaje desde la cuenta de alguien o en su nombre (incluyendo el uso de una dirección falsa en el campo 'De':).Si se autoriza por Dirección, una secretaria puede enviar emails en nombre de Dirección pero debería firmar el email en su propio nombre.
  - Sea razonable sobre el número y tamaños de email enviados y guardados. Periódicamente elimine del buzón correos antiguos o que no vaya a necesitar más y clasifique los mensajes que necesite para mantenerlos bajo las carpetas apropiadas.

POLÍTICAS DE SEGURIDAD:
POLÍTICA DE USO DE CONTRASEÑAS



- Todas las contraseñas del sistema (administradores, cuentas de administración de aplicaciones, etc.) deben ser cambiadas al menos una vez **cada tres meses.**
- Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas sin antes proceder a la identificación del interlocutor.
- Se evitarán nombres comunes, o cualquier otra combinación que pueda identificar al usuario (fecha nacimiento, matrículas de vehículos, etc.).

INCORRECTO

- **Pepitogarcia**
- **ab3421**
- **967 213423**

CORRECTO

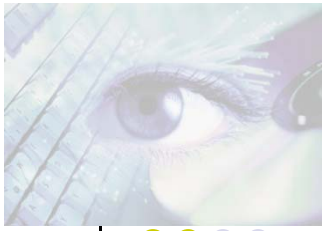
- **pgm4122**
- **xcp0x123**

OK

- Evitar la reasignación de identificadores de usuario redundantes.
- Utilización de un identificador único para cada usuario, de esta forma podrá vincularse a los usuarios y responsabilizarles de sus acciones.
- **No se accederá al sistema utilizando el identificador y la contraseña de otro usuario**. Las responsabilidades de cualquier acceso realizado utilizando un identificador determinado, recaerán sobre el usuario al que hubiera sido asignado.

Centro Europeo de Empresas e Innovación Albacete

POLÍTICAS DE SEGURIDAD:
POLÍTICA DE USO DE CONTRASEÑAS

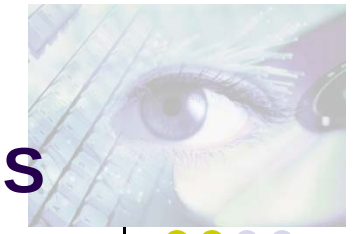


- **Utilice contraseñas de calidad, contraseñas "Fuertes":** La contraseña debe ser difícil de adivinar. Le damos algunas recomendaciones para crear contraseñas de calidad:
  - Evite palabras del diccionario. Es lo primero que busca cualquier sistema de detección de contraseñas.
  - No deben estar basadas en algo que le puede relacionar con usted, como fecha de nacimiento, nombre propio, etc.
  - No contengan caracteres consecutivos, idénticos, todos numéricos o todos alfanuméricos.

Características:

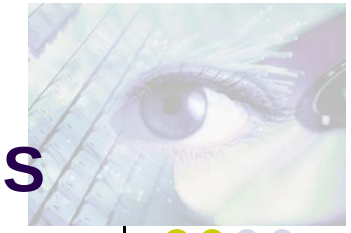
- Más de 7 caracteres (quince para seguridad completa).
- Utilice caracteres de tres de los cuatro grupos siguientes, SIEMPRE QUE UNO DE ELLOS SEA EL SÍMBOLO:
  - 1. Letras minúsculas.
  - 2. Letras mayúsculas.
  - 3. Números (por ejemplo, 1, 2, 3).
  - 4. Símbolos (por ejemplo, ¡, @, Ñ, =, -, etc.).
- No ser ni derivarse de una palabra del diccionario, de la jerga o de un dialecto.
- No derivarse del nombre del usuario o de algún pariente cercano.
- No derivarse de información personal (del número de teléfono, número de identificación, DNI, fecha de nacimiento, etc…) del usuario o de algún pariente cercano.

POLÍTICAS DE SEGURIDAD:
POLÍTICA DE USO ADECUADO DE PORTÁTILES



- Dejarse a la vista o abandonarse en lugares donde puedan ser sustraídos con facilidad.
- Cuando se vaya a dejar desatendido un portátil durante un periodo largo de tiempo, por ejemplo, por una reunión o ir a desayunar, el usuario debe:
- Cerrar la puerta de su despacho o área con llave si esta opción es posible.
- En situaciones vulnerables como lugares públicos, salas de espera de aeropuertos, hoteles o salas de conferencia, el portátil no debe dejarse nunca desatendido.
- No deben guardarse equipos portátiles en bolsas o maletas que puedan revelar que contienen elementos de valor en su interior para no atraer a ladrones.
- Cuando las medidas anteriores no puedan aplicarse por ser inviables o inapropiadas, el propietario del equipo es responsable de adoptar todas las medidas y precauciones que considere razonables con el objetivo de minimizar los riesgos de daño o robo del equipo.
- Un usuario deberá notificar al Responsable de Área, de forma inmediata la pérdida o robo del equipo entregado a su custodia. Cuando un equipo portátil sea sustraído o extraviado, deberá denunciar el hecho inmediatamente a la Policía y notificar la incidencia Responsable de Área.

POLÍTICAS DE SEGURIDAD:
POLÍTICA DE USO ADECUADO DE PORTÁTILES

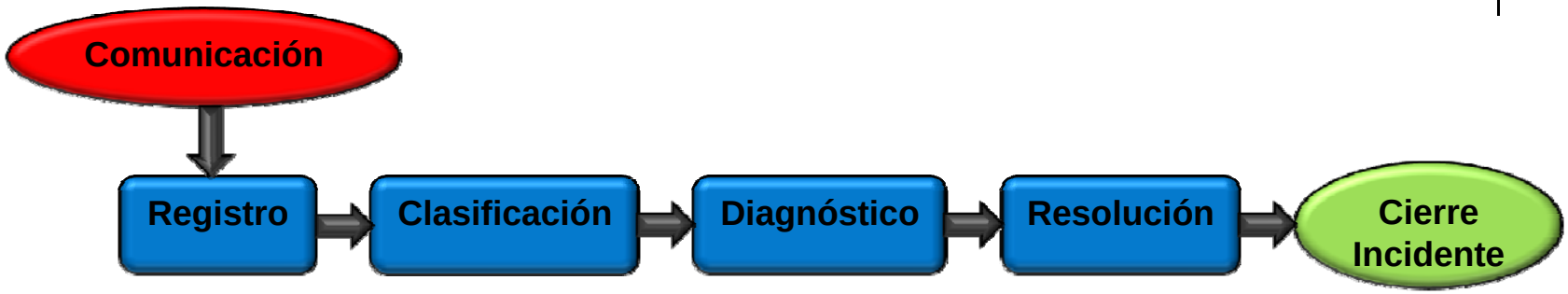


Acciones NO autorizadas:

- El intento de alterar, evitar o saltar las medidas de seguridad informática configuradas en el equipo entregado.
- La desconfiguración del equipo o la modificación del software preinstalado.
- La instalación de cualquier software sin autorización expresa y sin justificación asociada a necesidades laborales para el desempeño de una tarea productiva relacionada con las actividades de la organización.
- El uso del correo electrónico o Internet para finalidades distintas a las estrictamente profesionales relacionadas con el desempeño habitual de las funciones como empleado de la organización.
- La conexión a los sistemas de información de la organización sin las adecuadas medidas de seguridad en el equipo portátil.
  - No tener actualizado el software antivirus
  - No haber instalado los últimos parches de seguridad del sistema operativo.
- La conexión a Internet desde el equipo portátil a través de redes inalámbricas no acreditadas.

Centro Europeo de Empresas e Innovación Albacete

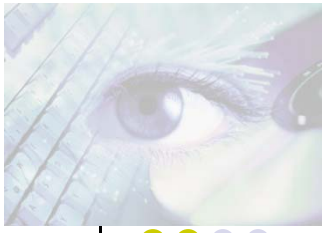
GESTIÓN DE INCIDENCIAS



OBLIGACIÓN DEL PERSONAL

NOTIFICAR LAS INCIDENCIAS AL DPTO. INFORMÁTICO

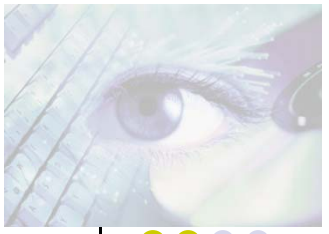
GESTIÓN DE INCIDENCIAS



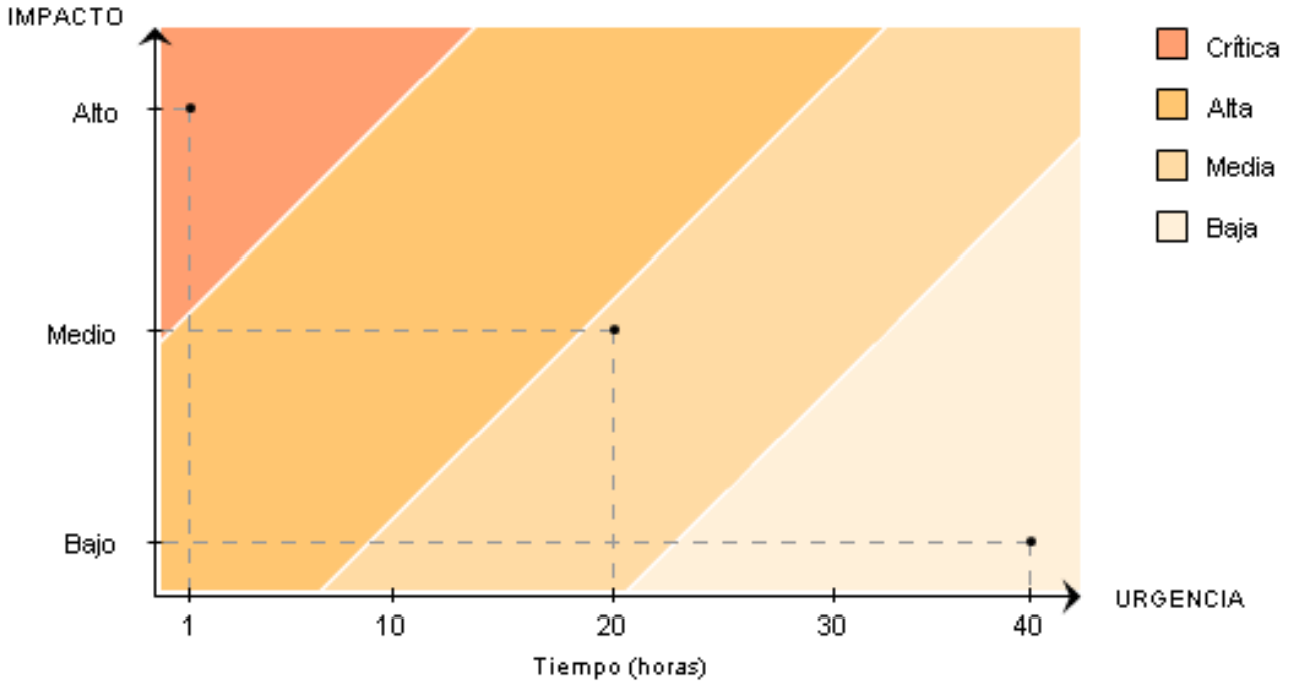
Posibles incidentes o eventos, que serán inexcusablemente registrados (esta lista no debe entenderse como Limitativa, sino que podrá ser ampliada con cualquier otro tipo de incidencias que hubiera quedado omitida) pueden ser los siguientes:

- pérdida de servicio, equipos o instalaciones
- fallos o sobrecargas del sistema
- errores humanos
- incumplimiento de políticas o directrices
- incumplimientos de los acuerdos de seguridad física
- cambios del sistema no controlados
- fallos del software o del hardware
- violaciones de acceso
- eventos que afecten a la identificación y autenticación de los usuarios
- eventos que afecten a los derechos de acceso a los datos
- incidencias que afecten a la gestión de soportes
- eventos que afecten a los procedimientos de copias de seguridad y recuperación.

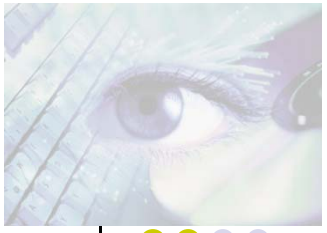
GESTIÓN DE INCIDENCIAS



Prioridad según Impacto y Urgencia



GESTIÓN DE INCIDENCIAS



- **Crítica:** Una emergencia es un incidente cuya resolución no admite demora. Los incidentes de este tipo se procesarán en paralelo de haber varios, y en su resolución se emplearán todos los recursos disponibles.
  - Ejemplo: todos los que supongan peligro para vidas humanas, para la infraestructura de Internet. Hasta ahora también se han considerado todos aquellos incidentes que requerían acción inmediata debido a su rapidez y ámbito de difusión.

- **Alta:** Un incidente de alta prioridad es aquél cuyas características requieren que sea atendido antes que otros, aunque sea detectado posteriormente. Para esto se mantiene una cola independiente de incidentes de alta prioridad, y no se procesarán los de prioridad inferior mientras queden de éstos. Los incidentes de alta prioridad se procesan en serie.

  - Ejemplo: se consideran incidentes de alta prioridad todos aquellos en que exista infiltración de una cuenta privilegiada o denegación de servicio.

- **Media:** Por defecto, los incidentes se atienden en serie por orden de llegada, mientras no requiera atención uno de prioridad superior. Un incidente de prioridad normal puede adquirir la categoría de alta prioridad si no recibe atención por un tiempo prolongado.

  - Ejemplo: todos los incidentes no clasificados como alta prioridad o emergencia, donde el atacante haya ganado acceso a un sistema informático ajeno. También se incluyen escaneas insistentes de redes.

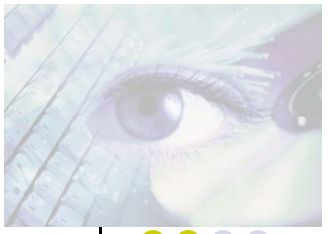
- **Baja:** Los incidentes de baja prioridad se atienden en serie por orden de llegada, mientras no requiera atención uno de prioridad superior. Un incidente de baja prioridad será cerrado automáticamente si no recibe atención por un tiempo prolongado.

Centro Europeo de Empresas e Innovación Albacete

Centro Europeo de Empresas e Innovación
Albacete

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS



- **SGSI.** La parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

- **Seguridad de la información.** Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

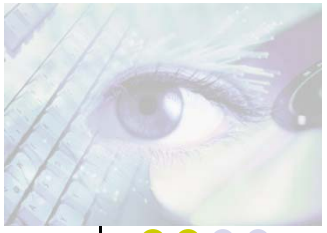
- **Auditoria**. Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

- **Amenaza.** Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Riesgo**. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

- **Riesgo Residual**. El riesgo que permanece tras el tratamiento del riesgo.

GLOSARIO DE TÉRMINOS



- **Política de seguridad.** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- **Plan de tratamiento de riesgos**. Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

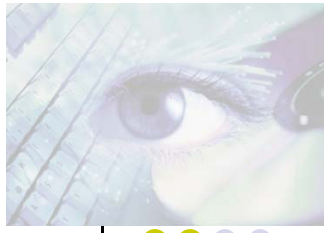
- **Selección de controles**. Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

- **Vulnerabilidad.** Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

- **Valoración de riesgos.** Proceso completo de análisis y evaluación de riesgos.

- **Tratamiento de riesgos.** Proceso de selección e implementación de medidas para modificar el riesgo

GLOSARIO DE TÉRMINOS



- **No conformidad**. Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

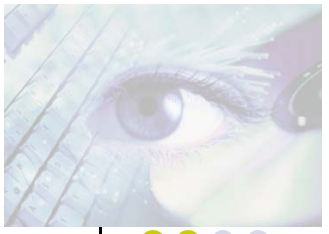
- **No conformidad grave**. Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

- **ISO 27001.** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable.

- **Inventario de activos**. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **Integridad**. Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

GLOSARIO DE TÉRMINOS

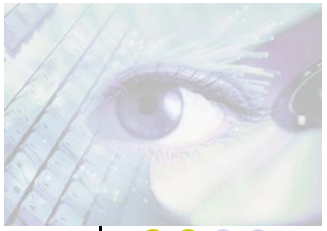


- **Incidente.** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Impacto**. El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros - pérdida de reputación, implicaciones legales, etc.

- **Gestión de riesgos**. Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.
- **Evento.** Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

GLOSARIO DE TÉRMINOS



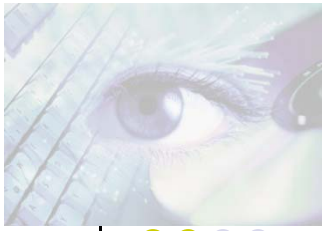
- **Evaluación de riesgos.** Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

- **Disponibilidad.** Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

- **Desastre**. Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

- **Control.** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. También se utiliza como sinónimo de salvaguarda o contramedida.

GLOSARIO DE TÉRMINOS



- **Control correctivo**. Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

- **Control preventivo**. Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

- **Control disuasorio**. Control que reduce la posibilidad de materialización de una amenaza.

- **Control detectivo**. Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

!! Gracias !!

Centro Europeo de Empresas e Innovación
Albacete