GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

GUÍA

EDUCANDO EN SEGURIDAD TI

Preventivos

marzo 2012

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format).

Se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección Accesibilidad > Formación > Manuales y Guías de la página http://www.inteco.es.

ÍNDICE

1. INTRODUCCIÓN

Hoy día, podemos afirmar sin temor a equivocarnos, que las organizaciones y las empresas, pueden aprovechar las tecnologías de la información en su beneficio, pero también debemos ser conscientes de los riesgos y amenazas asociados al uso de estas tecnologías y conocer la forma en que las empresas y las organizaciones pueden enfrentarse a ellas.

Alcanzar un adecuado nivel de seguridad es una tarea que pasa por desarrollar acciones en los distintos ámbitos de la materia, como son el **técnico**, el **jurídico o normativo** y el **organizativo**. Pero además, las organizaciones y las empresas, las componen personas y las estas son uno de los eslabones más importantes de la cadena de la seguridad y también uno de los más débiles. Es por ello qué, implantar seguridad en las organizaciones, pasa necesariamente por la **formación e información** a todas las personas que forman parte de la organización, independientemente del tamaño de esta y del perfil al que pertenezca.

No importa si se trata de un autónomo, de una empresa de 5 empleados o de una multinacional con miles de trabajadores repartidos por todo el mundo, todos deben disponer de la información adecuada a su responsabilidad, sobre aspectos relacionados con la seguridad, de forma que puedan desempeñar su actividad sin poner en peligro los activos de la organización.

A lo largo de este informe, desarrollaremos dos conceptos muy importantes, como son las buenas prácticas y las políticas de seguridad, dos herramientas fundamentales para **informar y formar** en seguridad TIC.

Esperamos que este informe / guía, ayude a las empresas y en especial a las pymes, a desarrollar acciones sencillas pero muy eficaces, que apenas requieren inversión, y que pueden ayudar a mejorar el nivel de seguridad de forma muy significativa.

2. ENFOQUES DE SEGURIDAD

La seguridad como concepto ha evolucionado a lo largo del tiempo, comenzando con el enfoque de **seguridad informática**, cuyo alcance estaba limitado a la protección de los sistemas e infraestructuras, otorgándoles un gran protagonismo, por encima de otros activos, como la información.

La seguridad informática, carecía de metodologías y criterios para el diseño, selección y aplicación de medidas de seguridad. En este enfoque, se consideraba que, a través de herramientas y medios técnicos era posible detener o minimizar cualquier amenaza, alcanzando un nivel de seguridad, que en muchas ocasiones, estaba por encima de las necesidades reales de la organización o cuyas medidas eran implantadas sin un criterio claro o adecuado.

Con la proliferación de las redes de comunicaciones, el abaratamiento del acceso a Internet y la aparición de los dispositivos portátiles, la naturaleza y ámbito de los sistemas a proteger cambió, lo que trajo consigo una evolución del concepto de seguridad, que fue sustituido por la **seguridad de las tecnologías de la información y las comunicaciones** o seguridad TIC.

Este nuevo enfoque supuso una mejora sustancial respecto al anterior, puesto que no solo incorporaba nuevos sistemas e infraestructuras, como aquellas destinadas a las comunicaciones, sino que además, otorgaba más importancia a la información como activo, por encima de otros. Así mismo, comenzaron a desarrollarse metodologías para el diseño, selección e implantación de medidas de seguridad y la seguridad cada vez tenía más importancia dentro de las organizaciones.

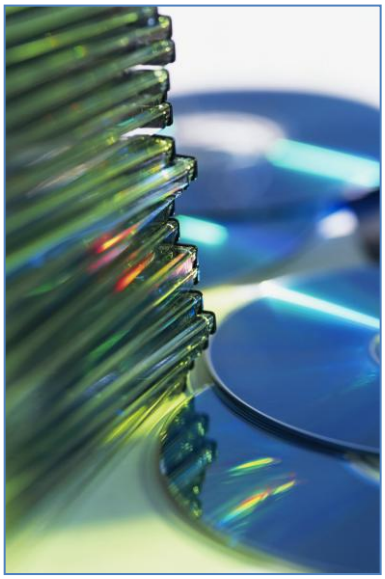
Poco a poco la seguridad comenzó a salir de los departamentos técnicos y de sistemas, para convertirse en un elemento integrado en cualquier actividad o proceso de negocio. Por otro lado, la aparición de normativa y legislación relativa a las tecnologías de la información, impulso el desarrollo del concepto de seguridad jurídica, así como la seguridad desde un punto de vista organizativo.

Finalmente, todo ello se integró en un concepto nuevo, mucho más amplio y cuya característica principal es considerar la información como el activo de mayor importancia y en torno al cual se desarrolla toda una metodología con un único objetivo, proteger la información.

A continuación podemos ver un sencillo diagrama que muestra la evolución que ha seguido, de forma muy simplificada, el concepto de seguridad.

Tal y como se ha indicado, la seguridad de la información desarrolla el concepto de seguridad en torno al activo más importante de cualquier organización: **la información.** A través de una metodología relativamente sencilla pero muy completa, se diseñan y seleccionan las medidas de protección adecuadas, de acuerdo con criterios de importancia de los activos a proteger, nivel de amenaza y riesgo al que están expuestos.

A través de esta metodología se busca alcanzar un nivel de seguridad adecuado y suficiente para la organización, de forma progresiva, a través de fases o ciclos, en cada una de las cuales va mejorando el nivel de seguridad hasta alcanzar el nivel deseado.



Una vez alcanzado dicho nivel, es necesario mantenerlo, ya que las organizaciones cambian y evolucionan en el tiempo, junto con su entorno, lo que supone que, una organización que consideramos “segura” en el momento actual, no tiene porque serlo dentro de un año.

Por todo ello, en la actualidad hablamos de **Sistemas de Gestión de la Seguridad de la Información (SGSI)**, de forma que la seguridad es entendida como un sistema de gestión y como parte de un proceso de mejora constante.

A lo largo de este documento vamos a tratar uno de los ámbitos a los que hace referencia la seguridad de la información, el organizativo, y concretamente vamos a ver dos herramientas muy interesantes y efectivas, que pueden ayudar a las empresas y organizaciones a alcanzar un nivel de seguridad adecuado, pero también a mantenerlo: las buenas prácticas y las políticas de seguridad.

3. ACCIDENTALMENTE O INTENCIONADAMENTE

La mayoría de los incidentes de seguridad que se producen dentro de las organizaciones se originan en los propios empleados por dos motivos principalmente: **desconocimiento o de forma intencionada**.

El desconocimiento es una de las principales causas detrás de buena parte de los incidentes de seguridad, pero en ocasiones el empleado sabe perfectamente lo que está haciendo y de hecho, con su forma de proceder, está buscando provocar un incidente de seguridad, motivado por la venganza o el beneficio económico.

En relación con lo anterior, a través de los siguientes apartados vamos a ver algunos casos que suelen darse en las organizaciones y que de una u otra forma, suelen derivar en incidentes de seguridad.

3.1. DESCONOCIMIENTO Y BUENAS PRÁCTICAS

El desconocimiento supone un riesgo potencial para la seguridad de las organizaciones. El desconocimiento deriva en un uso inadecuado e ineficaz de los recursos, pero sobre todo, es fuente de todo tipo de incidentes de seguridad. El desconocimiento está asociado a la falta información y formación por parte de los empleados.

Por otro lado, la ausencia de buenas prácticas, supone que es el empleado por sí mismo, el que debe de dar los pasos adecuados y realizar las actividades de la mejor forma posible, procurando no poner en riesgo la seguridad de la organización, lo cual, por desgracia, es demasiado suponer.

Ejemplos de incidentes cuyo origen está en el desconocimiento o en la falta de buenas prácticas podemos encontrarlos en situaciones tan habituales como consultar el correo electrónico o en el uso de las memorias USB en el entorno laboral. Es habitual que un empleado, en el desempeño de su actividad se encuentre con mensajes que parecen legítimos y auténticos, pero que contienen algún tipo de código malicioso, de forma que el ordenador acaba siendo infectado.

El 'spam' supone el 80% del tráfico del correo electrónico

El correo electrónico se ha convertido en un elemento indispensable en el día a día. Sin embargo, y precisamente por este uso masivo y universal, también se ha convertido en un peligroso cebo con el que los ciberdelincuentes intentan estafar a sus víctimas en busca de toda clase de datos personales, especialmente los vinculados a tarjetas de crédito y cuentas corrientes (más información)

Fuente de la noticia: eleconomista.es

El uso de los dispositivos USB es otra fuente de amenazas, como el robo de información, o la introducción de todo tipo de código malicioso. De hecho, se sabe por estudios realizados, que un elevado porcentaje de memorias USB, están infectadas y muchos usuarios lo desconocen.

Un 66% de las memorias USB extraviadas son portadoras de virus

Según Sophos, más de dos tercios de estas memorias están infectadas con malware y además tienen información privada sin cifrar. Algo que para esta compañía de seguridad es "preocupante", pues, significa que nadie entre los propietarios había utilizado ningún tipo de cifrado para proteger dichos archivos de "terceras personas" ante posibles extravíos o robos (más información).

Fuente de la noticia: RTVE

Proporcionar un conjunto de normas básicas sobre el adecuado uso de las infraestructuras que pone a disposición del empleado la organización, es uno de los medios para conseguir mejorar la seguridad y es una declaración de intenciones de la propia organización para con sus empleados, sobre la necesidad de hacer un uso adecuado y correcto de las infraestructuras.

3.2. INCUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD

En ocasiones el empleado, sabe perfectamente lo que está haciendo, conoce las buenas prácticas, y aún así, estas no son tenidas en cuenta. Cuando esto sucede, es necesario ir un paso más allá, y las organizaciones necesitan establecer políticas de seguridad, de forma que se establezcan claramente los límites y las normas que se deben cumplir, promoviendo un uso adecuado de los recursos e infraestructuras, sin poner en peligro la seguridad de la organización.

Si no existe una política de seguridad, entonces, el empleado, no dispondrá de normas y no conocerá los límites asociados a su actividad, lo que dejará un vacío, que podrá ser aprovechado para realizar todo tipo de actividades que pueden poner en peligro la seguridad de la organización.

Un ejemplo muy habitual de incumplimiento de las políticas de seguridad lo encontramos en el uso de las infraestructuras para actividades personales, como es el caso del acceso a las redes sociales en el entorno laboral. Además de la merma para la productividad, las redes sociales se han convertido en una vía de entrada para código malicioso y otras amenazas, a través de los miles de juegos, perfiles falsos y bulos que pululan en estas redes. De hecho, las organizaciones y las empresas son conscientes de este riesgo, como se desprende de la noticia siguiente.

El 76% de las empresas españolas prohíbe a sus empleados acceder a las redes sociales

El bloqueo es incluso mayor que la media europea, que muestra que el 72% de las empresas se protege de esta manera de las amenazas para la seguridad informática que las redes sociales representan, junto con los servicios de intercambio de archivos.

Según los resultados de un estudio realizado por la compañía de seguridad Kaspersky, el 56% de los responsables de informática está en contra del uso de las redes sociales en la empresa (más información)

Fuente de la noticia: Criptex

La mensajería instantánea o el uso del correo electrónico para uso personal, son también prácticas habituales en las empresas, que supone un importante riesgo para la seguridad.

La mensajería instantánea se confirma como una herramienta peligrosa para la seguridad de las empresas

Un estudio de Symantec confirma que el 60% de los trabajadores que usan mensajería instantánea en el trabajo lo hace para contactar con usuarios fuera de su organización. Además un 43% lo utiliza para compartir contenido que no tiene relación con el trabajo, por lo que la posibilidad de introducir contenidos peligrosos es bastante elevada (más información).

Fuente de la noticia: CSO Spain

Lo cierto es que la mayoría de los empleados son conscientes de la violación de las políticas de seguridad y peor aún, lo hacen de forma regular, tal y como se desprende de la siguiente noticia.

7 de cada 10 empleados suelen violar las políticas de seguridad de su empresa

En un reciente informe elaborado a pedido de la firma Cisco, se entrevistó a 2800 personas sobre sus usos y costumbres a la hora de la seguridad digital. Y pocos cumplen con las reglas de seguridad.

El trabajo de investigación es el "Cisco Connected World Technology Report" y ente los muchos datos relevados se destacan los siguientes:

De aquellos empelados jóvenes que si son conscientes de las políticas de seguridad respecto a la tecnología, el 70% (globalmente) admitió haber roto las

políticas de seguridad impuestas con variada regularidad. (más información)

Fuente de la noticia: Criptex

A todo ello hay que sumarle el hecho de que, por desgracia, en el trabajo solemos buscar la comodidad y la facilidad, lo cual en ocasiones va en contra de la seguridad. En otras ocasiones, las políticas de seguridad no son adecuadas o no contemplan actividades habituales que pueden poner en grave riesgo la seguridad, pero que se sabe, se realizan de forma habitual en la organización.

El 62% de las empresas europeas pierden datos confidenciales, por el extravío de memorias USB desprotegidas

La mayoría de las compañías no incluye el control de estos dispositivos de memoria en sus políticas de protección de datos.

Diario Ti: Kingston Digital Europe ha anunciado los resultados de su estudio "El Estado de la Seguridad de Memorias USB en Europa" realizado por el Ponemon Institute con la finalidad de establecer cómo las empresas gestionan los requerimientos de seguridad y privacidad de la información recogida y almacenada en las memorias USB. El estudio confirma que muchas ignoran el riesgo de no utilizar memorias USB encriptadas y no siguen una política de seguridad apropiada para estos dispositivos. (más información)

Fuente de la noticia: Zona Virus

3.3. EL PROBLEMA DE LOS EMPLEADOS VIP

Un empleado VIP es aquel que posee más privilegios dentro de la estructura o jerarquía de la organización, debido a su cargo, o nivel de responsabilidad.

Es importante aclarar que las buenas prácticas y las políticas de seguridad hacen referencia a todos los empleados, con independencia de su categoría o nivel en la escala de la organización, otra cosa es como se apliquen o en que difieran en función del puesto o del nivel de responsabilidad.

Uno de los principales problemas de seguridad asociados a los empleados VIP, es que suelen tener acceso a información confidencial o sensible, como planes estratégicos, información de productos en desarrollo, información operativa o diversa documentación interna. Debido a la información a la que tienen acceso, el incumplimiento de las políticas de seguridad o de las buenas prácticas, puede suponer un grave problema de seguridad, que puede derivar en un incidente de seguridad con gran impacto sobre el neoocio.

Los altos directivos deberían implicarse directamente en la ciber-seguridad

Un informe advierte del riesgo y las pérdidas económicas que supone para las organizaciones no introducir a ejecutivos de nivel C en cuestiones relacionadas con la seguridad cibernética. La seguridad informática es un serio problema que puede costar a las empresas mucho dinero. Sin embargo, aún hoy las altas esferas lo consideran únicamente una cuestión de TI. (más información)

Fuente de la noticia: CSO España

Por otro lado, es muy importante que la dirección y los responsables de la organización cumplan y den ejemplo en lo que se refiere al cumplimiento de las políticas de seguridad y las buenas prácticas, de forma que el resto de los empleados conozcan la implicación de la dirección y esto suponga un incentivo para el cumplimiento por parte de todos.

En los últimos años, la responsabilidad corporativa en la seguridad de las organizaciones ha cobrado enorme importancia. De hecho, en la actualidad se suele considerar como un paso fundamental, en la implantación de seguridad en la organización, conseguir la implicación de la dirección o gerencia, independientemente del tamaño de la organización.

En los siguientes apartados vamos a conocer un poco más sobre las buenas prácticas y las políticas de seguridad.

4. BUENAS PRACTICAS Y POLÍTICAS DE SEGURIDAD

Las buenas prácticas son un conjunto de recomendaciones generales, relativas a seguridad, que toda empresa debería de incorporar a su operativa diaria. Se trata de un documento que refleja un conjunto de normas básicas, que todos los empleados de la organización deben conocer, desde la dirección o gerencia, hasta los trabajadores de menor nivel en la escala o jerarquía de la organización, y lo más importante, **todos deben hacer lo posible para cumplirlas e integrarlas en su actividad diaria**.

El documento de buenas prácticas puede hacer referencia a múltiples aspectos relacionados con seguridad y se diferencia de la política de seguridad, en que no es de obligado cumplimiento, y por otro lado, suelen ser un conjunto de normas de alto nivel, que se pueden aplicar a todo tipo de escenarios, organizaciones y situaciones.

A continuación vamos a ver un modelo de documento de buenas prácticas, con algunos ejemplos de las recomendaciones que podemos encontrar en este tipo de documento.

Buenas practicas

Ejemplo de documento de buenas prácticas:

- Usar contraseñas robustas y cambiarlas de forma regular.
- No instalar programas o aplicaciones que no estén relacionados con la actividad laboral.
- No utilizar el correo electrónico para el envío o recepción de datos personales.
- No conectar dispositivos USB al puesto de trabajo.
- No utilizar la mensajería instantánea en el horario de trabajo.
- No conectarse a redes sociales o mensajería instantánea en el horario del trabajo.
- No utilizar la dirección de email del trabajo para darse de alta en servicio de Internet que no estén relacionados con la actividad laboral.

Ejemplo de documento de buenas prácticas en seguridad TIC

Al contrario que las buenas prácticas, las políticas de seguridad, son normas que suelen estar diseñadas, al menos en parte, para una organización en concreto y situaciones especificas, de forma que, una política puede ser adecuada para una organización, y en cambio para otra no.

Además, las políticas se pueden diseñar a varios niveles, por ejemplo, puede haber una política de seguridad general para toda la organización, pero luego, pueden existir otras más especificas, que hacen referencia a procesos concretos, o procedimientos específicos relacionados con una actividad determinada.

Política de contraseñas

Un ejemplo de política específica es la política de contraseñas, la cual puede establecer los siguientes puntos o requisitos que se deben de cumplir:

- Las contraseñas deben de ser generadas usando un algoritmo, es decir, de forma automatizada.
- Las contraseñas deberán de tener una longitud mínima de 8 caracteres.
- Las contraseñas deberán de incluir como mínimo los siguientes grupos de caracteres:
  - Letras mayúsculas y minúsculas.
  - Números.
- Las contraseñas deberán de ser cambiadas cada 3 meses (ver procedimiento de renovación de contraseña)

Ejemplo de política de seguridad.

Las políticas suelen ser de obligado cumplimiento y de hecho, cada vez es más habitual que cuando un empleado es contratado por una empresa, uno de los documentos que debe conocer y leer detenidamente es precisamente, la política de seguridad. En muchos casos, aunque depende de la organización, la política de seguridad debe de ser aceptada por el empleado, para lo cual, firma el documento, indicando de esta forma su conformidad con los contenidos y comprometiéndose a su cumplimiento.

El contenido de las políticas de seguridad se refiere a lo que supone que debe de cumplirse, pero no describen cómo debe de hacerse, para ello están los procedimientos de seguridad, que detallan los pasos a seguir en cada procedimiento, de forma que además, estos procedimientos cumplan en todo momento la política de seguridad.

Finalmente, ya sea que se trate de buenas prácticas o de políticas de seguridad, es fundamental que todos los empleados las conozcan, ya sea en el momento de su incorporación a la organización, o durante el tiempo que dure su actividad en esta. Si se producen cambios o modificaciones, será necesario difundir los documentos actualizados a toda la organización. **El valor de las buenas prácticas y las políticas está precisamente en que todos los miembros de la organización las conozcan.**

5. DOCUMENTO DE BUENAS PRACTICAS

A continuación proporcionamos un conjunto normas generales que pueden formar parte de cualquier documento de buenas prácticas. Todas las empresas y organizaciones, deberían de contar al menos con un documento de buenas prácticas con los siguientes puntos que se indican a continuación.

Ámbito de aplicación	Descripción
Generales	✓ Para cualquiera de las aplicaciones y servicios usar contraseñas robustas y cambiarlas de forma regular. ✓ No instalar programas o aplicaciones que no estén relacionados con la actividad laboral. ✓ No utilizar el correo electrónico para el envío o recepción de datos personales. ✓ No conectar dispositivos USB al puesto de trabajo. ✓ No utilizar la mensajería instantánea, o servicios de redes sociales. ✓ Realizar copias de seguridad de forma regular.
Correo electrónico	✓ No utilizar la dirección electrónica de empresa para darse de alta en sitios web o servicios que no estén relacionados con la actividad laboral. ✓ No confiar en correos electrónicos de dudosa procedencia. ✓ No abrir documentos adjuntos sin comprobar el remitente y el contenido del correo electrónico. ✓ No enviar información sensible o confidencial a través del correo electrónico, sino es estrictamente necesario.
Navegación web	✓ No acceder a sitios o contenidos no relacionados con la actividad laboral. ✓ No descargar aplicaciones o contenidos de sitios dudosos o de poca confianza. ✓ Para la tramitación o el envío de información sensible o confidencial a través de formularios utilizar siempre un protocolo seguro HTTPS.

Tal y como se ha comentado, las buenas prácticas no son de obligado cumplimiento, pero su difusión a todos los empleados, supone que todo están informados y si se produce un incidente o se detecta algún tipo de actividad que vulnere alguno de los puntos que se indican en el documento de buenas prácticas, el empleado no podrá alegar desconocimiento o falta de información por parte de la empresa.

Además, las buenas prácticas son un primer paso para el establecimiento de políticas y procedimientos específicos de seguridad y también son el punto de partida para establecer un conjunto de normas básicas que todos los empleados deberían de cumplir.