

La ciberseguridad como elemento clave en los procesos TD



Rocio Viruega Hernández

Gestora de Desarrollo de Negocio Smart TICs.

e-mail: rviruega@syltec.es

Linkedin: <https://www.linkedin.com/in/rocio-viruega-78247359/>





ENGINEERING
SYLTEC
Making the future





Instalaciones



Obra Civil



Transformación Digital



I+D+i





La ciberseguridad no es solo una cuestión técnica, es una responsabilidad compartida que requiere la atención de todos en la empresa.

Satya Nadella, CEO de Microsoft.

¿Qué es la transformación digital?

La Transformación Digital (TD) es un proceso mediante el cual las organizaciones utilizan la tecnología para mejorar significativamente el rendimiento, la eficiencia y la innovación en todos los aspectos de sus operaciones. Este cambio no se trata solo de adoptar nuevas herramientas tecnológicas, sino de cambiar fundamentalmente la forma en que una organización opera y ofrece valor a sus clientes.



Portal web y redes sociales



Que debemos tener en cuenta:

- **Proveedor:** garantías de seguridad, sellos, auditorias... que utilicen métodos de desarrollo seguro a la hora de construir nuestra web.
- Disponer de un certificado digital **SSL (HTTPS://)**
- Garantizar **acceso seguro** al panel de administración
- **Copias de seguridad** periódicas
- Mantener el gestor de contenidos **actualizado**
- Medios de **pago seguros** (tienda online)
- Registros de la actividad generada

Portal web y redes sociales



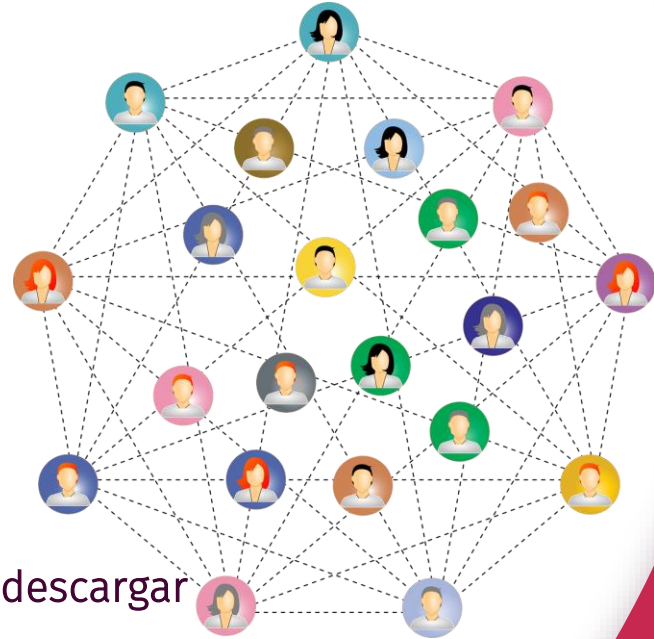
Podemos evitar:

- Denegación del servicio
- Defacement
- Sustracción de datos
- Ataques phishing
- Almacenamiento y distribución de malware

Portal web y redes sociales

Que debemos tener en cuenta:

- Contraseñas robustas
- Habilitar el **doble factor de autenticación**
- Configuración de **privacidad**
- Normas de publicación
- Restricciones de acceso
- **Phising y malware**
- Precaución a la hora de seguir **enlaces y descargar adjuntos**
- Evitar **errores humanos**



Teletrabajo



Teletrabajo seguro

- Normativa y procedimentación
- Control de los usuarios que pueden trabajar en remoto y a que aplicaciones y recursos tiene acceso
- Formación , concienciación
- Priorizar el uso de equipos corporativos
- Periodo de implantación y pruebas

Teletrabajo seguro

- **Acceso seguro:** contraseñas robustas y doble autenticación y cambio periódico de las mismas
- Configuración de los equipos
- Cifrado de los soportes de información y copias de seguridad
- Conexiones seguras VPN
- Evitar la conexión de redes públicas
- Aplicaciones de teleconferencia y colaborativas

Incidentes más frecuentes

1 de cada 4
fraude online*

*Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro.

16.902 incidentes son **phishing***



***Phishing.**

Correo electrónico que simula ser una entidad legítima con el objetivo de robar información privada, realizar un cargo económico o infectar el dispositivo.



***Ransomware.**

Secuestro de datos de un dispositivo.



***Malware.**

Software malicioso que lleva a cabo acciones como extracción de datos u otro tipo de alteración de un sistema.

tiendas online fraudulentas

654 tiendas fraudulentas cerradas durante el año 2022.

+14.000
malware*
448 incidentes son
ransomware*



4 de cada 10
sistema vulnerable*

*Sistema operativo de un dispositivo no actualizado o mal configurado.

+5.000
contenido abusivo*



*Pornografía infantil, delitos de odio, ciberacoso, etc.

Correo electrónico

- Normativa
- Correos sospechosos: Formación para identificar correos fraudulentos y comunicación
 - El contenido del mensaje muestra modificaciones visuales, como cambios en logotipos o pies de firma, en comparación con los mensajes previos recibidos de la misma fuente.
 - El mensaje incluye una "llamada a la acción" que nos insta, invita o solicita realizar alguna acción inusual.
 - Se nos pide que proporcionemos credenciales de acceso a un sitio web o aplicación, como información de cuenta bancaria o datos de un sistema.

Correo electrónico

- **Identificar el remitente.** Si dudamos llamamos por teléfono o contactamos por otra vía.
- **Análisis de correos adjuntos:** La descarga de archivos adjuntos maliciosos podría comprometer nuestros dispositivos con malware. Mantener el antivirus activo y actualizado es fundamental para detectar posibles amenazas.

Correo electrónico

Medidas para identificar que un archivo adjunto es malicioso:

- El nombre del archivo incita a descargarlo
- El icono no coincide con el tipo de archivo. A menudo los archivos ejecutables se ocultan bajo iconos de aplicaciones como Word, Excel o PDF.
- .rar. .zip
- Desconfía si te pide habilitar opciones desactivadas por defecto

Correo electrónico

Inspección de enlaces:

- Revisar la URL normalmente cuando situamos nuestro ratón encima del texto del enlace aparece la dirección del enlace antes de pinchar en él.
- Pueden tener letras o caracteres de más o de menos y que se parezca mucho al original

Correo electrónico



ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN ELECTRÓNICA.

informamos que está disponible una nueva notificación para obra@g-energy.es como Titular con los siguientes datos:

- Titular obra@g-energy.es
- Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: L02000050
- Identificador: 51452666411e4bf42a89
- Concepto: Notificación -- Expediente 4699/2021 (SIA 2087160, Serie SF0249)
- Vínculo: Titular

Se puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: <https://agenciatributaria.gob.es>

Facilitamos un enlace directo a la [notificación](#).

De acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la aceptación de la notificación o bien la presunción de rechazo por no haber accedido a la notificación durante el periodo de puesta a disposición, dará por efectuado el trámite de notificación y se continuará el

procedimiento de esta notificación por distintas vías electrónicas o incluso en papel por vía postal. Si accediera al contenido de esta notificación por más de una de estas vías, sepa que los efectos jurídicos empezarán a contar desde la fecha en que se produzca su primer acceso.

Madrid, a 15 de mayo de 2021

Correo electrónico

- Antimalware y antispam: instalación de aplicaciones antimalware y activar filtros antispam tanto en el servidor como en el cliente
- Cifrado y firma digital: protección de la información confidencial
- No responder al correo spam
- Usar BCC o CCO para el envío a múltiples destinatarios.

Cloud



Cloud

- La empresa debe determinar si permite el uso de servicios de almacenamiento en la nube pública. Los empleados deben adherirse a las regulaciones establecidas por la empresa.
- crear y difundir una lista de servicios de almacenamiento en la nube permitidos y prohibidos para evitar el uso de plataformas consideradas inseguras.
- Los empleados deben conocer qué tipo de información pueden almacenar en la nube, cuándo ciflarla y esto debe estar contemplado en la política de clasificación de información

Cloud

- Copias de seguridad en la nube, evaluar ventajas y desventajas .
- crear y difundir una lista de servicios de almacenamiento en la nube permitidos y prohibidos para evitar el uso de plataformas consideradas inseguras.
- Al contratar servicios de almacenamiento en la nube, es esencial asegurarse de que cumplen con criterios de seguridad específicos requeridos para la información a almacenar, como confidencialidad, disponibilidad y requisitos legales, especialmente en el caso de datos personales. Es importante entender la política de seguridad del proveedor.

Concienciación y formación



Concienciación y formación

La concienciación y formación en ciberseguridad son componentes críticos y fundamentales para la seguridad informática en las empresas.

Razones clave:

Amenazas Constantes:

- El panorama de amenazas cibernéticas evoluciona constantemente. La concienciación y formación aseguran que los empleados estén al tanto de las últimas amenazas y tácticas utilizadas por los ciberdelincuentes.

Concienciación y formación

Primera Línea de Defensa:

- Los empleados son la primera línea de defensa contra ataques cibernéticos. La concienciación les permite reconocer y reportar posibles amenazas, reduciendo el riesgo de caer en trampas o ser víctimas de ataques de ingeniería social.

Protección de Activos Digitales:

- La formación ayuda a los empleados a comprender la importancia de proteger los activos digitales de la empresa, incluidos datos confidenciales, propiedad intelectual y sistemas críticos. Esto contribuye a la integridad y confidencialidad de la información.

Concienciación y formación

Cumplimiento Normativo:

- Muchas industrias y regiones tienen requisitos normativos específicos en materia de ciberseguridad. La formación asegura que los empleados estén al tanto de estas regulaciones y cumplan con las prácticas recomendadas.

Prevención de Pérdidas Financieras:

- La concienciación sobre ciberseguridad reduce el riesgo de caer en estafas o ataques financieros. La formación puede incluir prácticas seguras para realizar transacciones en línea y evitar fraudes financieros.

Concienciación y formación

Cultura de Seguridad:

- Fomentar una cultura de seguridad en toda la empresa es esencial. La formación promueve la responsabilidad individual y colectiva en la protección de la empresa contra amenazas cibernéticas.

Reducción de Riesgos Humanos:

- Muchas violaciones de seguridad tienen un componente humano, como contraseñas débiles o prácticas inseguras. La formación ayuda a mitigar estos riesgos humanos, mejorando la postura general de seguridad.

Concienciación y formación

Reconocimiento de Amenazas

- La concienciación capacita a los empleados para reconocer señales de posibles amenazas, como correos electrónicos de phishing, sitios web maliciosos o dispositivos USB desconocidos, antes de que causen daño.

Respuesta Efectiva a Incidentes

- La formación proporciona conocimientos sobre cómo responder eficazmente a incidentes de seguridad, minimizando el impacto y ayudando en la recuperación.

Concienciación y formación

Protección de la Reputación de la Empresa

- Una violación de seguridad puede dañar la reputación de la empresa. La concienciación y formación ayudan a prevenir incidentes que podrían afectar la imagen y la confianza de los clientes y socios.

Concienciación y formación

La concienciación y formación en ciberseguridad son inversiones esenciales para fortalecer la postura de seguridad de una empresa y mitigar los riesgos asociados con las amenazas cibernéticas en constante evolución.

¡Gracias!



www.syltec.es
rviruega@syltec.es