OFICINA Acelera pyme

OTDR ACITICS

CIBER SEGURIDAD

Para PYMES y AUTÓNOMOS

Guía Práctica

Financiado por la Unión Europea
NextGenerationEU

red.es

Plan de Recuperación, Transformación y Resiliencia

Índice

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

Plan de Recuperación, Transformación y Resiliencia

01 Introducción a la Ciberseguridad

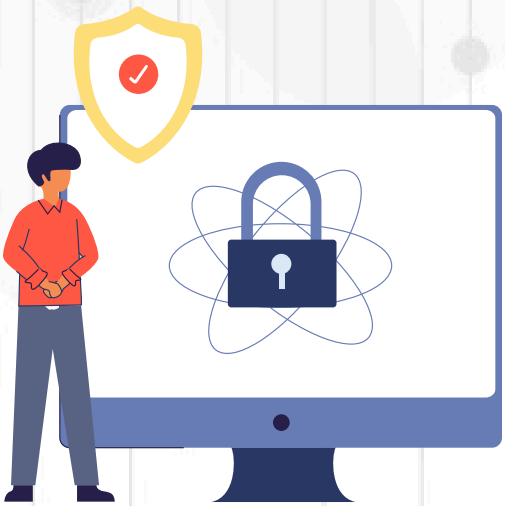
Entendemos por **Ciberseguridad** al conjunto de prácticas y procesos diseñados para proteger sistemas informáticos, redes y dispositivos de posibles ataques, daños o robos en línea. Su objetivo principal es garantizar la confidencialidad e integridad de la información en el entorno digital.

En un mundo cada vez más interconectado, donde la tecnología juega un papel crucial, la ciberseguridad se ha convertido en un factor esencial para proteger la información y garantizar el funcionamiento seguro de los sistemas.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

Cualquier empresa gestiona información que es de gran valor para la empresa, pero también para los ciberdelincuentes.
El objetivo estos ciberdelincuentes también incluyen los sistemas que gestionan esta información, ya que les permite gestionar estos perpetrar otros fraudes o incluso extorsionar a la empresa propietaria.

Esta guía tiene como objetivo proporcionar las recomendaciones básicas para protegerse en el mundo digital, por un lado identificando las amenazas más comunes a las que se enfrentan, y por otro lado, adoptando las medidas efectivas para combatirlas.



Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

02

Amenazas más comunes

RANSONWARE

Actúan sobre datos confidenciales impidiendo el acceso a sistemas claves. Solicitan un rescate económico para recuperar los datos y evitar la divulgación de los mismos.

PHISHING

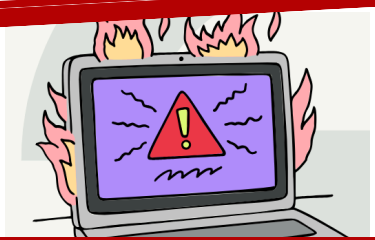
Suplantación de una entidad legítima (como un banco) para engañar y manipular al usuario y obtener sus datos o instalar programas que capturen sus credenciales.

Fuga de información

Pérdida de confidencialidad de la información de la empresa, debido a un incidente de seguridad que puede ser de forma voluntaria o involuntaria.

Suplantación de proveedor

El ciberdelincuente suplanta la identidad del proveedor y consigue que el empresario le realice una transferencia bancaria.



MALWARE

Software malicioso que puede dañar o inhabilitar dispositivos, robar información o espiar a los usuarios. Incluye virus, gusanos o troyanos

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

03

Protección ante amenazas

Proteger tus dispositivos ante las diferentes amenazas cibernéticas es imprescindible para mantener la información segura. Para ello son necesarias las siguientes medidas:

1- **Formación:** La formación del equipo es la principal herramienta para que tus empleados sean conscientes y se sientan parte responsable de la seguridad. Esta formación debe incluir la normativa de protección de datos que aplique a tu negocio.

2- **Protección de datos:** Implementar el cifrado de datos para proteger la información sensible y realizar periódicamente copias de seguridad de los datos críticos, almacenándolos en lugar seguro.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

3- <u>Seguridad de la red:</u> Implementar un firewall para evitar los accesos no autorizados a tu red y asegurarte de que la red Wi-fi esté protegida con una contraseña fuerte.

4- <u>Gestión de accesos:</u> Implementar un firewall para evitar los accesos no autorizados a tu red y asegurarte de que la red Wi-fi esté protegida con una contraseña fuerte.

5- <u>Actualizaciones:</u> Asegurarse de que tanto los sistemas operativos como las aplicaciones, incluidos antivirus y antimalware, estén actualizadas con los últimos parches de seguridad

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

6- **Monitoreo:** Implementar herramientas que monitoricen la actividad en la red y así poder detectar cualquier actividad sospechosa.

7- **Plan de Respuesta:** Desarrollar un plan de respuesta ante los posibles incidentes de seguridad, incluyendo cómo comunicarte con las partes afectadas.

8- **Evaluación de Riesgos:** Evaluar regularmente la seguridad de los sistemas y procesos para identificar posibles vulnerabilidades y asesorarse por profesionales en ciberseguridad.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

04 Gestión de Contraseñas y Acceso

La gestión de contraseñas y acceso es un aspecto crucial en la ciberseguridad. A continuación se detallan algunas de la prácticas recomendadas para asegurarse que las contraseñas y el acceso a los sistemas sean seguros.

Creación de Contraseñas Fuertes: Las contraseñas deben tener al menos una longitud de 12 caracteres, incluyendo mayúsculas, minúsculas, números y símbolos, evitando utilizar información personal en las mismas.

Gestores de Contraseñas: Se utilizan para almacenar y generar contraseñas complejas, únicas para cada cuenta.

Estos gestores deben tener opciones de sincronización segura entre dispositivos.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

Políticas de Contraseña: Establecer la obligación del cambio de contraseña cada cierto tiempo e implementar un sistema que bloquee la cuenta tras varios intentos fallidos de inicio de sesión.

Control de Acceso: Los empleados sólo podrán acceder a la información necesaria para poder realizar su trabajo. Asegurándonos que sólo las personas autorizadas tengan acceso a información sensible.

Monitoreo y Registro: Mantener un registro de acceso a los sistemas críticos para poder identificar movimientos sospechosos e implementar herramientas que monitoricen el acceso en tiempo real para detectar comportamientos inusuales.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

05

Respuestas y cumplimiento legal

Ante un ciberataque, es crucial saber qué debemos hacer para proteger los derechos de las personas afectadas y cumplir con la normativa vigente.

En cuanto a la respuesta, los pasos que debemos dar podemos resumirlos en los siguientes:

1- **Detección y análisis del ataque:** Una vez detectada una amenaza, debemos identificar qué tipo de amenaza es y cuál es el nivel de gravedad.

2- **Contención y erradicación:** Aislar los sistemas afectados, eliminando la raiz de la amenaza.
Implantar los parches de seguridad necesarios.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

3- Mitigación y Recuperación: Restaurar los sistemas afectados desde las copias de seguridad anteriores al incidente. Asegurarse de que todas las acciones de recuperación se ajustan a los requisitos legales y reglamentarios.

4- Mejora continua: Realizar análisis posteriores al incidente, con el fin de abordar las áreas susceptibles de mejora y actualizar el plan de respuesta periódicamente.

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

En cuanto al cumplimiento legal ante un ciberataque, debemos tener en cuenta las siguientes cuestiones.

1- **Protección de datos personales:** El Reglamento General de Protección de Datos (GDPR) de la Unión Europea establece que si se produce una violación de seguridad que afecte a los datos personales, se debe notificar a las autoridades en un plazo máximo de 72 horas posteriores al incidente.
La Agencia Española de Protección de Datos (AEPD) establece cómo gestionar estas situaciones y las obligaciones de los responsables del tratamiento de los datos.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

2- Obligación de notificación: Si el incidente compromete datos personales que comprometan los derechos y libertades de los afectados, el responsable del tratamiento de los datos debe informar a los mismos.
A veces es necesario comunicarlo a las personas afectadas, explicando qué datos se han visto comprometidos, cómo les puede afectar y qué medidas se están tomando.

3- Normativa específica: Existe normativa específica de ciberseguridad que se debe implementar en las empresas dedicadas a ciertos sectores económicos. Por ejemplo la Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) obliga a los prestadores de servicios.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

4- Investigación y consecuencias legales: Tras el ataque, puede ser necesaria una investigación que determine el origen y los responsables del mismo, que pueden enfrentarse a sanciones.

La empresa afectada también puede estar expuesta a acciones legales por negligencia si no a cumplido con la normativa aplicable.

5- Responsabilidad: Si el ataque ha causado daños económicos o personales a los usuarios, puede haber una responsabilidad civil por parte de la empresa que no tomó las precauciones necesarias, incluso en algunos casos podrá exigirse una responsabilidad penal.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

06

Conclusiones

La ciberseguridad es un aspecto crítico para cualquier negocio en el mundo digital actual. Implementar estas prácticas puede ayudar a proteger a tu empresa contralas diferentes amenazas cibernéticas y garantizar la seguridad de tus datos y los de tus clientes.

La ciberseguridad debe considerarse como una de las inversiones más importantes en una empresa, incluyendo la formación de los empleados, ya que la prevención ante este tipo de incidentes es la mejor herramienta evitarlos.

Si tienes más preguntas o necesitas más información sobre algún tema específico, ¡no dudes en preguntar!

Financiado por la Unión Europea
NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

OTDR ACITICS

OFICINA DE TRANSFORMACIÓN
DIGITAL PARA ENTORNOS RURALES

Financiado por
la Unión Europea
NextGenerationEU

red.es

Plan de
Recuperación,
Transformación
y Resiliencia