ESTRATEGIA DE CIBERSEGURIDAD DEL PRINCIPADO DE ASTURIAS

CONSEJERÍA DE PRESIDENCIA

DIRECCIÓN GENERAL DE SEGURIDAD Y ESTRATEGIA DIGITAL (DGSED)

“La Ciberseguridad debe acompañar cada ámbito del proceso de transformación digital de la Administración”

La estrategia de ciberseguridad se establece analizando la casuística de cada proceso de negocio en el que intervienen herramientas electrónicas. No hay fórmulas mágicas, sino la ejecución de múltiples medidas que sirven para minimizar los riesgos

CONTENIDOS

Recorrido por la Estrategia de Ciberseguridad

1 **CONTEXTO**

Organización de la gestión de la ciberseguridad en el Principado de Asturias.

2 **OBJETIVO**

Establecer los objetivos mínimos en la estrategia de defensa frente a ciberataques

3 **PRIORIDADES, INICIATIVAS y LÍNEAS DE ACCIÓN**

Detalle sobre cómo conseguir estos objetivos, trabajando por prioridades estratégicas en iniciativas concretas y líneas de acción.

4 **PRINCIPALES RIESGOS**

Dificultades para la implementación efectiva de la estrategia, así como los riesgos existentes

1. Contexto

Organización de la ciberseguridad en la Administración del Principado de Asturias

La base: Recursos Dedicados

La Dirección General de Seguridad y Estrategia Digital tiene dentro de sus competencias, entre otras, la dirección, diseño, desarrollo, implantación, mantenimiento y gestión de los programas y políticas de seguridad en materia de sistemas de información **para todos los ámbitos de la Administración del Principado de Asturias**.

Servicio de Seguridad y Datos

Ejerce las funciones de dirección, diseño, desarrollo, implantación y mantenimiento de los programas y políticas de seguridad en materia de sistemas de información para **todos los ámbitos de la Administración del Principado de Asturias**.

Le corresponde el control de riesgos en sistemas de información, la puesta en marcha de medidas correctivas para su reducción, así como la redacción y seguimiento del cumplimiento de normativas y estándares que se desarrollen en materia de tecnologías de la información y comunicaciones. Asimismo, es el responsable de la actualización y aplicación de los procedimientos, procesos y metodologías que aseguren la calidad, tanto de los productos como de los servicios que se presten.

Se encarga de definir la arquitectura de bases de datos más adecuada a la política de gestión del dato en el Principado de Asturias y establece los modelos de normalización y eficiencia en el almacenamiento de los datos de todos los ámbitos de la Administración del Principado de Asturias. Asimismo, genera los cuadros de mando necesarios para dar respuesta a las necesidades de gestión y diseña las políticas de explotación de los datos.

También tiene a su cargo la definición, desarrollo y evolución de aquellos programas informáticos que sean transversales e integradores para el resto de sistemas y aplicaciones existentes en la Dirección General.

Centro de Gestión de Servicios Informáticos (CGSI)

Este servicio da soporte, operación, administración, documentación, evolución, adaptación y gestión de cada uno de los componentes sobre los que se desarrollan y ejecutan los sistemas de información, servicios de negocio y soporte del Principado de Asturias, incluidos en el Catálogo de la Administración del Principado de Asturias.

Uno de los lotes del mismo se encarga, específicamente, de la resolución de incidencias, problemas y cambios en materia de seguridad TIC; administración de sistemas de gestión de identidad y de gestión de acceso a los sistemas TIC, diseño e implantación de infraestructuras y herramientas de seguridad, soporte técnico en materia de seguridad y la participación activa en los procesos ITIL implantados, así como la realización y el mantenimiento de la documentación asociada y la participación en la gestión y ejecución de actuaciones y proyectos que requieran adaptar y/o evolucionar estos servicios.

La ciberseguridad dentro de cultura de la organización

Las metodologías de trabajo, certificaciones o el cumplimiento de normas van más allá de meros reconocimientos. Son demostraciones de una cultura organizativa en la que se fomentan las buenas prácticas.

Este es el mejor camino para minimizar los riesgos.

La Certificación en el Esquema Nacional de Seguridad no es un objetivo en sí misma, sino una forma de obligarnos a mantener las buenas prácticas.

En el Principado acabamos de renovar la certificación ENS de nivel medio en los Sistemas de Información que dan soporte a la Sede Electrónica

2. Objetivo

Objetivos frente a potenciales ciberataques

Minimizar daños

Todas las organizaciones han sufrido y/o sufrirán impactos por algún tipo de ciberataque. Lo más importante es que los daños originados sean los mínimos posibles

01

Minimizar el número de incidentes

Mediante diferentes medidas de prevención y herramientas de protección

02

Minimizar el alcance de los mismos

Estableciendo barreras de protección entre diferentes redes y sistemas de información

03

Minimizar el impacto

A través de modelos de recuperación de datos

3. PRIORIDADES, INICIATIVAS y PROYECTOS

Cómo conseguir los objetivos, prioridades estratégicas y líneas de acción

Alineamiento estratégico

- **Crecer en organización con otras administraciones**
- **Colaboración con el Estado**
- **Integrarse en la red nacional de socs**
- **Apoyarse en herramientas y conocimiento del CCN**
- **Enfoque de recomendaciones INCIBE:**
  Medidas de ciberseguridad desde una perspectiva global | INCIBE-CERT

Mantenimiento, evolución e impulso de IA en las herramientas:

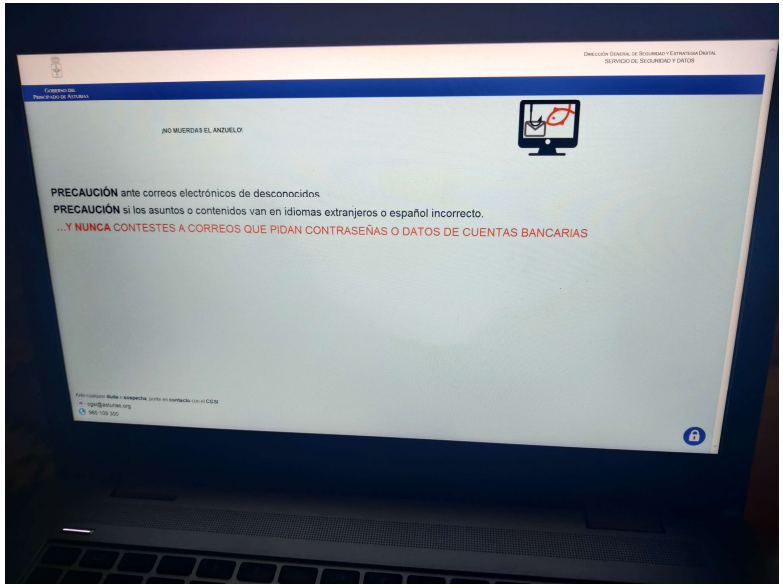
Siem
Waf
Proxy
Anti malware

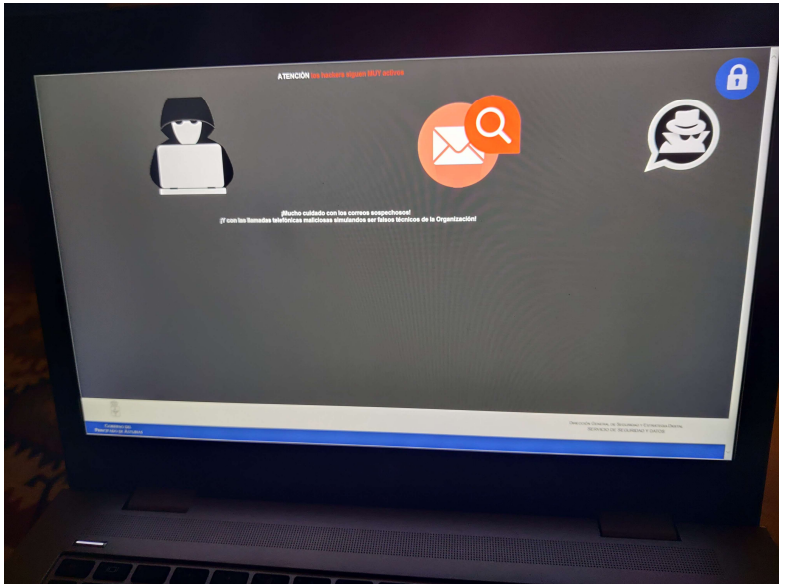
Anti ddos
Firewalls
Protección de correo
Ips
Etc, …

Reforzar la identidad digital, el control de los accesos remotos, el uso de dobles factores, la formación y la concienciación de usuarios

Algunos ejemplos de prevención…

ATENCIÓN: Este correo electrónico proviene de fuera de la organización. Sea muy cauto, e incluso ignore, los enlaces y archivos adjuntos que aparecen en el mismo, especialmente si desconoce al remitente u observa algún indicio de posibles contenidos maliciosos. Es esencial recordar que NUNCA DEBE INTRODUCIR SUS CONTRASEÑAS COMO RESPUESTA A UN CORREO.





4. RIESGOS DE LA ESTRATEGIA

Retos a superar

Desde diferentes ángulos

Escasez de talento

No hay suficientes profesionales formados en el ámbito de la ciberseguridad para cubrir todas las necesidades del mercado

Mantener el nivel

Las amenazas evolucionan muy rápido y debemos aguantar el ritmo evolucionando las políticas de seguridad

Presupuesto

El mantenimiento de las políticas requiere una inversión continuada y determinada capacidad presupuestaria

Funcionalidad

Se debe mantener un equilibrio entre seguridad y funcionalidad

ASTURIAS,
TERRITORIO DIGITAL

DIRECCIÓN GENERAL DE SEGURIDAD Y ESTRATEGIA DIGITAL (DGSED)