

Ciberseguridad en el Sector Postal

**Dirección Nacional de Telecomunicaciones y Servicios de Comunicación
(DINATEL)**

Ec. María José Franco
mariajose.franco@miem.gub.uy

URSEC

Jornada Anual

Regulación de los Servicios de Comunicaciones, 17 de octubre de 2024



Ministerio
**de Industria,
Energía y Minería**

¿Qué es la ciberseguridad?

Para el Instituto Nacional de Estándares y Tecnología (NIST/EEUU), la ciberseguridad es la **prevención** de daños, explotación, uso no autorizado y restauración de sistemas electrónicos de información y comunicaciones.



IBM dice que refiere a cualquier tecnología, medida o práctica para **prevenir ciberataques o mitigar su impacto.**

ISACA: la Ciberseguridad es **la protección de los activos de información,** abordando las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados.

Objetivo



Reforzar la integridad, confidencialidad y disponibilidad de los sistemas de información.

Proteger los sistemas, las aplicaciones, los dispositivos informáticos, los datos confidenciales y los activos de las personas y las organizaciones contra ataques.



¿Por qué es importante la Ciberseguridad en el sector postal?

- Naturaleza sensible de la información que se maneja: datos personales, datos financieros, identificación de domicilio.
- Los sistemas postales están altamente conectados para facilitar la comunicación y la circulación de los envíos postales a través de las redes.
- Procesos y productos digitalizados. Ej. Tracking, Giros, etc.
- El crecimiento exponencial del comercio electrónico, donde aumenta la exposición de los clientes a entornos digitales.
- Es necesario construir confianza en toda la cadena, con socios; clientes; proveedores de servicios de transporte; aduanas; etc.



Incidentes de ciberataques en el sector postal

- Denegación de servicios: se sobrecargan los sistemas provocando interrupciones de los servicios en línea.
- Secuestro de dominios: se cifran los datos de una organización exigiendo rescate para liberarlos.
- Infección con malware, los hackers pueden usar archivos maliciosos para causar fallas en el sistema o el servidor.
- Phishing: a través del correo electrónico, mensajes de texto, u otras formas de comunicación para robar información sensible.
- Suplantación de identidad (spoofing): se hace pasar por una entidad legítima para cometer fraude.

Según Google, el 43% de los ciberataques son a pymes

Se estima que España sufre cerca de 30.000 ciberataques al año, con las pymes como eslabón más débil, pues son el objetivo de siete de cada diez de estos ataques.

U.S. Postal Service Confirms Data Breach

Employee, Customer Information Potentially Compromised

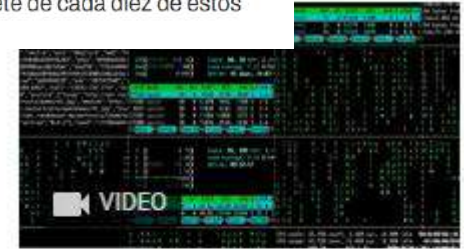
jeffrey Roman · @gen_sed · November 10, 2014 ·

Share Tweet Share Credit: Engle



The Federal Bureau of Investigation is leading an investigation into a **data breach** at the **U.S. Postal Service**, which affected employees and customers.

See Also: Webinar | Identity Crisis: How to



Intendencia de Paysandú aún no puede cobrar contribución tras ciberataque

El ataque también impactó en el pago a los trabajadores, aunque esa situación ya se ha solucionado.

18 DE AGOSTO DE 2024

04/11/2024

El hacker y especialista en ciberataques uruguayo, Mauro Eldritch, aseguró que un grupo de ransomware (hackers que se dedican a robar información, pedir rescates o luego venderla) liberó 77 gigabytes de datos robados tras un ciberataque a la empresa Geocom que administra terminales POS en Uruguay.

El Uruguayo advierte sobre circulación de SMS y correos electrónicos fraudulentos

bre la circulación de mensajes de texto (SMS) y correos de carácter fraudulento, que suplantán la identidad de Correo uruguayo al destinatario que debe realizar diferentes acciones, por lo que se actualizan su dirección, para recibir un supuesto envío a su nombre.



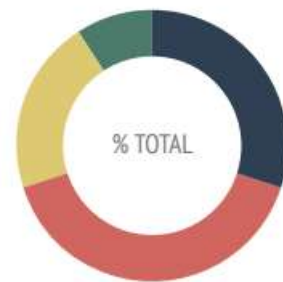
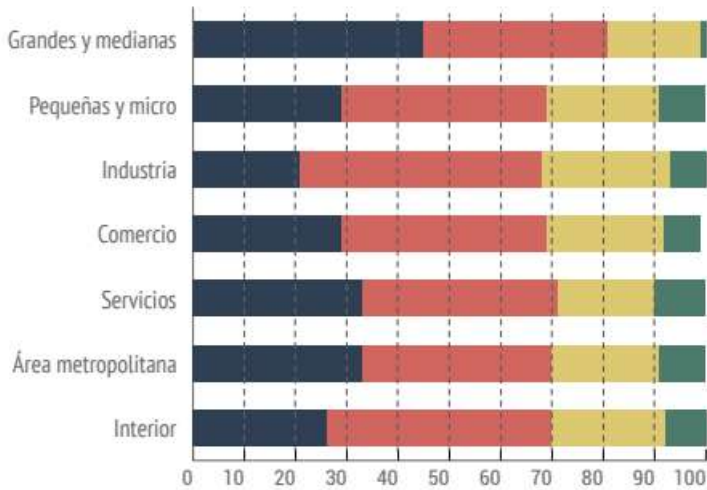
Ministerio
de Industria,
Energía y Minería

Encuesta de Datasec en colaboración con Grupo Radar, 2024.

¿Cuánto le preocupa a su empresa los incidentes en seguridad de información?

Ejemplo: virus, hackeos, correos fraudulentos, robos o secuestros de información.

BASE 1



30%
Me preocupa muchísimo

40%
Me preocupa bastante

21%
Me preocupa un poco

9%
No me preocupa nada

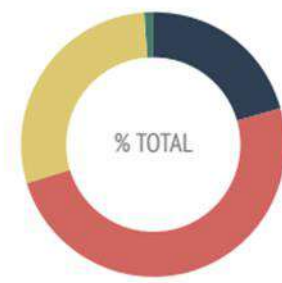
2022

35%

43%

15%

7%



21%
Sí, completamente

50%
Sí, parcialmente

29%
No

1%
No sabe

2022

34%

41%

23%

2%

2021

29%

35%

29%

7%

Preocupa la brecha entre la percepción y la preparación

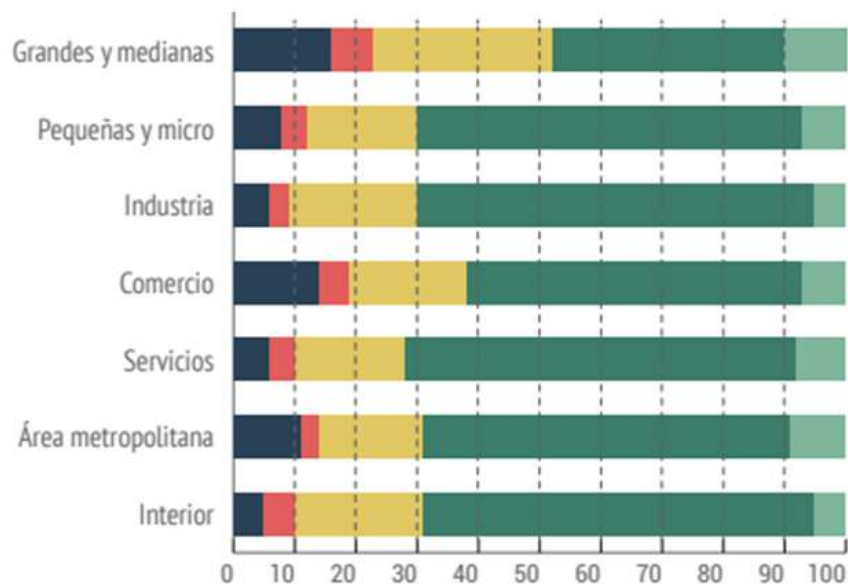
21% de las empresas encuestadas consideran haber tomado medidas suficientes



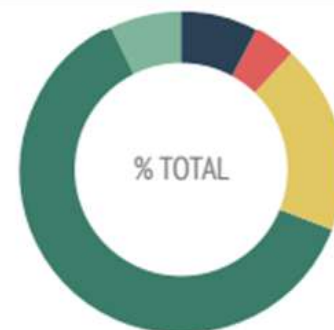
Ministerio de Industria, Energía y Minería

¿Se ha realizado algún tipo de evaluación del estado de su Ciberseguridad?

BASE 1



— Datasec



Ministerio
de Industria,
Energía y Minería

Posicionamiento de Uruguay en ranking internacional. UIT, Global Cybersecurity Index report 2024.

Uruguay

GCI 5th Edition Country Performance



Country Score

out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures
19.15	20	19.51	19.45	16.58

*Countries are classified according to www.itu.int

Area(s) of Relative Strength

Technical Measures
Capacity Development Measures
Organizational Measures
Legal Measures

Area(s) of Potential Growth

Legal Measures
Cooperation Measures

Tier Performance

T2: Advancing



Ministerio
**de Industria,
Energía y Minería**

Marco Normativo

Artículo 78 - Ley 20.212 del 6/11/2023

Las **entidades públicas y las entidades privadas** vinculadas a servicios o sectores críticos del país, deberán:

- Adoptar medidas de seguridad eficaces para proteger sus activos de información críticos, de conformidad con los lineamientos indicados AGESIC.
- Designar un responsable de seguridad de la información y comunicarlo a AGESIC.
- Planificar la adopción de las medidas para mitigar y mejorar los controles existentes.
- Adoptar las medidas de prevención que determine la reglamentación.
- Informar al CertUy la existencia de incidentes de Ciberseguridad.
- Incorporar, en función de su nivel de madurez, el marco de ciberseguridad desarrollado por AGESIC.
- Dar cumplimiento a otras medidas que determine el Poder Ejecutivo a efectos de proteger los activos de información, siguiendo los estándares nacionales e internacionales en la materia.

Se atribuye a AGESIC el cometido de desarrollar, promover la implantación y monitorear una estrategia nacional de ciberseguridad.

Se faculta a AGESIC a adoptar medidas con respecto a las entidades que incumplan con las obligaciones establecidas.



Marco de Ciberseguridad del NIST

Guía diseñada para ayudar a las organizaciones a gestionar y reducir los riesgos asociados a la digitalización.

Se compone de 3 partes claves: núcleo, nivel de implementación y perfiles.

Núcleo: identificar, proteger, detectar, responder y recuperar.

Niveles: evalúan las prácticas de seguridad de las organizaciones.

1. Parcial: medidas de seguridad reactivas
2. Repetible: políticas y procedimientos
3. Adaptable: enfoque proactivo, procesos que se adaptan y mejoran.

Perfiles: se adapta el marco para cada vertical, identificando debilidades y priorizando la gestión del riesgo.



AGESIC: define los lineamientos a nivel nacional

- Marco de Ciberseguridad: Conjunto de requisitos y buenas prácticas que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.
- Guía de implementación: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-implementacion/guia-implementacion-0>
- Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTUy): trabaja en el monitoreo, prevención, coordinación y respuesta a incidentes de ciberseguridad.
- Herramienta de autoevaluación en Ciberseguridad: <https://uruguay.iadb-tools.org/index.html?pais=URY>
- Reportar un incidente al CERTUy: a través del formulario de reporte de incidente, por mail a cert@cert.uy; telefónicamente al número (+598) 2 901 2929 Extensión 8567



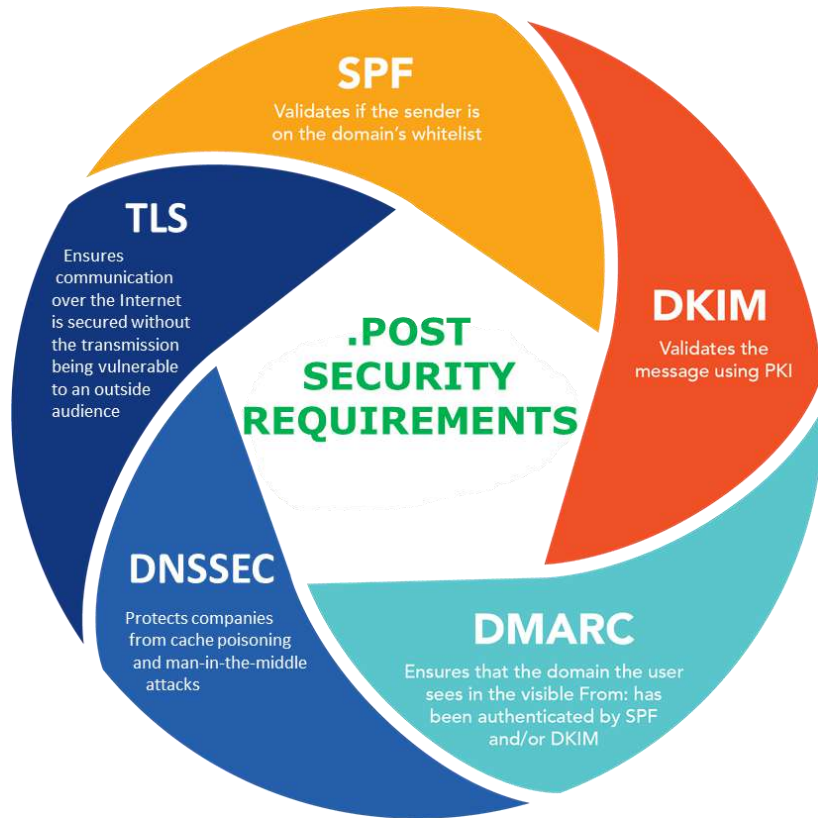
Otros Recursos

ISO 27.001

- Objetivo gestionar la Seguridad de la Información en una empresa.
- Aplica a cualquier tipo de empresa sin importar su tamaño y actividad.
- La base está en la importancia que tiene la dentro de la organización como elemento fundamental para cumplir con los objetivos.
- La información es un activo.
- Propone un **Sistema de Gestión para la Seguridad de la información** que se compone de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomando como base los riesgos que pueden poner en riesgo la información en una empresa u organización.



Marco de Cibseguridad de la Unión Postal Universal



- El gráfico representa diferentes capas y funciones que el sector postal debe incluir en sus procesos para cumplir con la ciberseguridad.
- Implica desarrollar medidas de protección en los puntos de acceso a la red, las oficinas postales: firewalls, políticas de acceso y autenticación.
- Alienta el uso de diferentes verificaciones en la comunicación entre los proveedores de servicios y el cliente.
- Pone a disposición Recomendaciones y Guías que pueden ser consultadas:

<https://www.upu.int/en/universal-postal-union/activities/digital-services/post-domain/security-policy>



Cyberdrills de la Unión Internacional de Telecomunicaciones

La UIT apoya a los países en su preparación, protección y capacidad de respuesta a incidentes en materia de ciberseguridad mediante la realización de cbersimulacros dinámicos a nivel regional y nacional.

Impulsa las capacidades de respuesta a incidentes. Los cbersimulacros se constituyen como una plataforma para la colaboración, el debate, para compartir prácticas e identificar los desafíos emergentes en materia de ciberseguridad.

Apoya en el desarrollo e implementación de procedimientos operativos efectivos. Ofrecen ejercicios prácticos para los equipos de respuesta a incidentes informáticos, impulsando mejoras tangibles en sus estrategias de preparación y respuesta.

Fortalece la cooperación internacional entre los Estados miembros, garantizando esfuerzos sostenidos y unificados para contrarrestar las amenazas cibernéticas.



Estructura de los Cyberdrills <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx>

Los días 1 y 2 - sesiones dinámicas de desarrollo de capacidades y talleres, incluidos los centrados en la protección de infraestructuras críticas, protección de la niñez en línea, estrategias de ciberseguridad y debates internacionales sobre estos temas.

El día 3 - paneles de discusión sobre evaluaciones y tendencias emergentes en amenazas a la ciberseguridad.

Los días 4 y 5 - se centran en la simulación de incidentes cibernéticos del mundo real (escenarios inmersivos). Los participantes abordan una serie de ataques de alto impacto, elaborados por expertos en la plataforma Cyber Range. Los participantes tienen el desafío de investigar, analizar y desarrollar estrategias de mitigación efectivas.

Objetivo: perfeccionar habilidades, validar políticas y enriquecer planes, procedimientos y procesos, para contribuir a el aseguramiento, a la preparación, prevención, respuesta, recuperación y continuidad de las operaciones.



Gracias

**Dirección Nacional de Telecomunicaciones y Servicios de Comunicación
(DINATEL)**

Ec. María José Franco
mariajose.franco@miem.gub.uy
Tel. 2840 1234 int 5106



**Ministerio
de Industria,
Energía y Minería**