chec
Grupo•epm
PROYECTO CENTINELA: SEGURIDAD UNA ASUNTO DE TODOS
Contribuir a la armonía de la vida
para un mundo mejor

Proyecto Centinela

Seamos GUARDIANES de nuestra información

chec | Grupo·epm

Análisis del entorno: Materialidad y Principales Riesgos Globales

Temas Materiales Grupo EPM

- Solidez financiera
- Tarifas y precios
- Acceso y comprabilidad
- Calidad y seguridad de productos y servicios
- Clima organizacional
- Contratación Responsable para el desarrollo local
- Derechos Humanos
- Transparencia
- Agua y biodiversidad
- Estrategia climática
- Energías renovables

Top Riesgos Globales 2021

WORLD ECONOMIC FORUM

- Crisis de medios de vida - Pobreza
- Clima Extremo
- Fracaso de la acción climática
- Crisis de recursos naturales
- Crisis de deuda
- Estancamiento Prolongado
- Enfermedades infecciosas
- Crisis de deuda
- Estancamiento Prolongado
- Migración Involuntaria
- Erosión de la cohesión social
- Clima Extremo
- Fracaso de la acción climática
- Daño ambiental humano
- Pérdida de biodiversidad
- Crisis de recursos naturales
- Fallo de ciberseguridad
- Avería de la infraestructura de TI
- Desigualdad digital
- Fractura de relaciones interestatales

Económico | Ambiental | Geopolítico | Social | Tecnológico

CIBER + SEGURIDAD

Proyecto Centinela | Seamos GUARDIANES de nuestra información

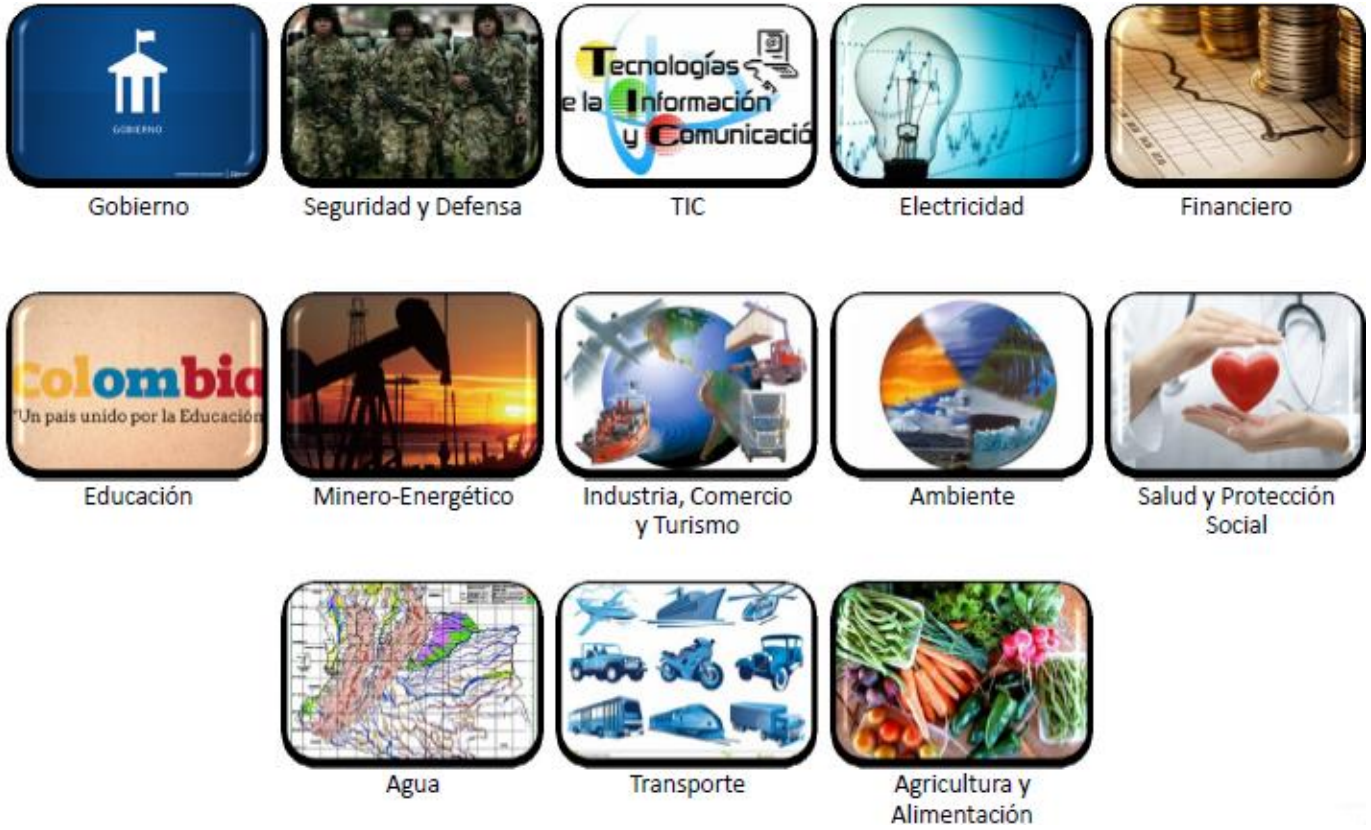
La ciberseguridad es el conjunto de acciones y maniobras destinadas a **proteger equipos informáticos y conexiones en red ante posibles ataques.**

Infraestructuras críticas en Colombia

Infraestructuras | Críticas

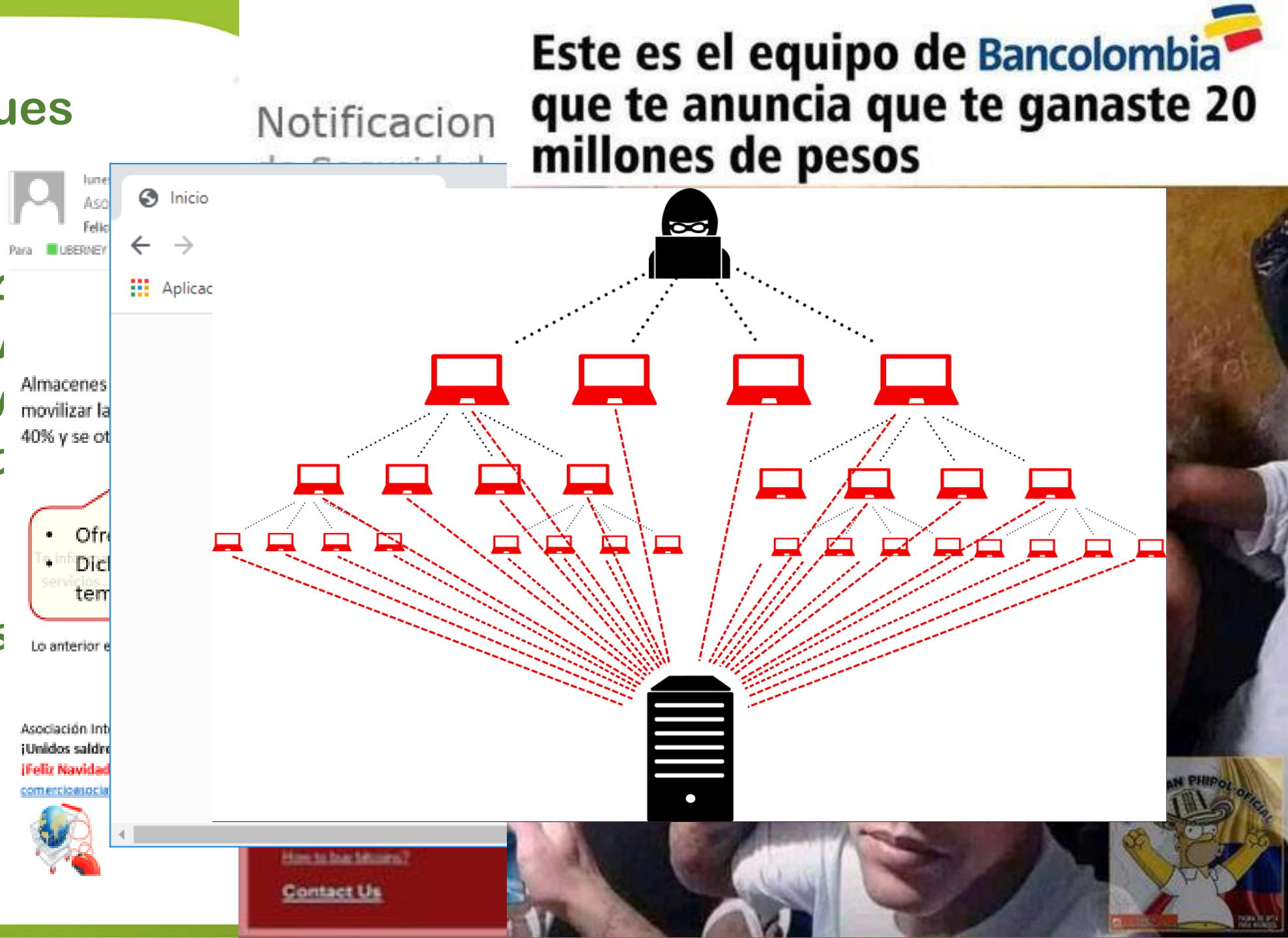
Servicios esenciales

"Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales."



Tipos de ataques

- *Phishing*
- *Suplantacio*
- *Ransomwa*
- *Cryptojack*
- *SQLInjectio*
- *DDoS*
- *Malware*
- *Ciberextors*



Algunos datos interesantes

Proyecto Centinela | Seamos GUARDIANES de nuestra información

SGSI

ISO 27001

ACUERDO CNO-1347

cno
Consejo Nacional de Operación

OBJETIVO

Desarrollar la capacidad organizacional de ciberseguridad y resiliencia en la organización, con el fin de tener una operación sostenible de los negocios de manera segura, protegiendo la infraestructura critica y la prestación de los servicios que ofrece, y protegiendo la información crítica para los diferentes grupos de interés

Implementar una guía de ciberseguridad en:

- Plantas de generación > 20 MW
- Subestaciones > 115 KVA
- Centro de control
- EDAC (Esquema de Desconexión Automático de Carga)

¿Proveedores & Contratistas?

Proyecto Centinela | Seamos GUARDIANES de nuestra información

Acceso a Información Organizacional Clasificada Y reservada/ tratamiento de datos Personales.

Desarrolla, implementa o provee sistemas de Información para TI /TO

Presta servicios en nube

Presta servicios de Ingeniería o diseño de soluciones de TO que Involucran ciberactivos críticos

Acceso a instalaciones con infraestructura crítica para TI/TO

Qué controles de seguridad tiene implementados en la empresa?

Hardware: firewall, IPS/IDS, bloqueo USBs

Software: Antivirus, control de navegación, contraseñas fuertes, MFA, restricción para descargar e instalar programas

Procesos: Políticas, Procedimientos, Estándares, Buenas prácticas

Personas: Sensibilización frente a los riesgos de ciberseguridad, capacitación, investigación de antecedentes, acuerdos de confidencialidad antes y después del contrato laboral

Política de seguridad de la información y ciberseguridad

CHEC se compromete en proteger la información, los activos críticos y ciberactivos que posee, con el fin de contar con información integra, completa y con los niveles de confidencialidad requeridos para la toma de decisiones, la operación segura y la respuesta oportuna a incidentes o ataques sobre sus activos críticos y ciberactivos, de forma que se garantice la continuidad en la prestación de los servicios.

(Febrero/2017)

✓ Lineamientos

- Protección de información, activos críticos y ciberactivos
- Mantenimiento del inventario de activos críticos y ciberactivos
- Respuesta oportuna a incidentes o ataques
- Continuidad del negocio y resiliencia
- Competencia y concienciación

Seguridad digital y continuidad de los servicios de tecnología

Tips generales:

- Usar contraseñas fuertes
- No reciclar contraseñas
- Cambiar las contraseñas cada mes
- No llamar “contraseñas”, al archivo donde anoto las contraseñas, usar KeyPass.
- No abrir enlaces o adjuntos de correos que no conozco
- No usar apps gratuitas
- No usar memorias USBs
- Tener herramientas de protección licenciadas
- Implementar prácticas de desarrollo seguro

IIS 10.0 Detailed Error - 4

localhost/weblog/bogus

HTTP Error 404.0 - Not Found

The resource you are looking for has been removed, had its name changed, or is temporarily unavailable.

Most likely causes:

- The directory or file specified does not exist on the Web server.
- The URL contains a typographical error.
- A custom filter or module, such as URLScan, restricts access to the file.

Things you can try:

- Create the content on the Web server.
- Review the browser URL.
- Create a tracing rule to track failed requests for this HTTP status code and see which module is calling SetStatus. For mor tracing rule for failed requests, click here.

Detailed Error Information:

Module	IIS Web Core	**Requested URL**	http://localhost:80/weblog/bogus
Notification	MapRequestHandler	**Physical Path**	C:\projects2010\West Wind Web Log\WebLog\bogus
Handler	StaticFile	**Logon Method**	Anonymous
Error Code	0x80070002	**Logon User**	Anonymous

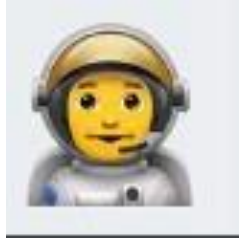
More Information:

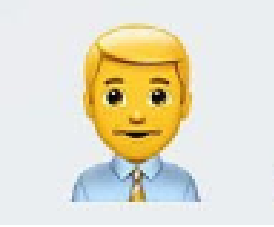
This error means that the file or directory does not exist on the server. Create the file or directory and try the request again.
View more information »

Seamos GUARDIANES de nuestra información

RIC de Gestión de incidentes de seguridad

Proyecto Centinela | Seamos GUARDIANES de nuestra información





seguridadinfo@chec.com.co

correosospechoso@epm.com.co

Proyecto Centinela | Seamos GUARDIANES de nuestra información

chec | Grupo-epm

“La conciencia del peligro, ya es la mitad de la seguridad y de la salvación”.

Ramón J. Sénder

¿Si un hacker decidiera atacar la información o los sistemas de su organización, estaría preparado?

¿Podría responder correctamente a un ataque?

Proyecto Centinela

Seamos GUARDIANES de nuestra información

Gracias!

chec | Grupo·epm