Ciberseguridad en operaciones

Marzo 2018

gnacio Lagomarsino.
ert@cert.uy
nacio.lagomarsino@cert.uy

agesic
DESARROLLANDO EL URUGUAY DIGITAL

PRESIDENCIA
República Oriental del Uruguay

Misión de CERTuy

Servicios

Reactivos

- Coordinación
- Respuesta de incidentes
- Análisis forense
- Evaluacion de amenazas

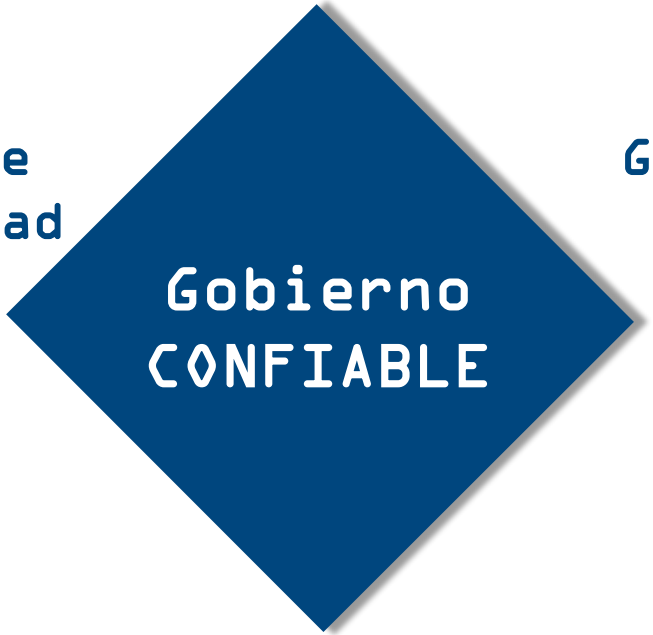
Proactivos

- Escaneos de vulnerabilidades
- Hackeos Eticos
- Despliegue y desarrollo de sensores.
- Recomendaciones y buenas prácticas

V.A.

- Capacitación y Entrenamiento

Agenda de Ciberseguridad



Ecosistema de Ciberseguridad

Identificación Electrónica

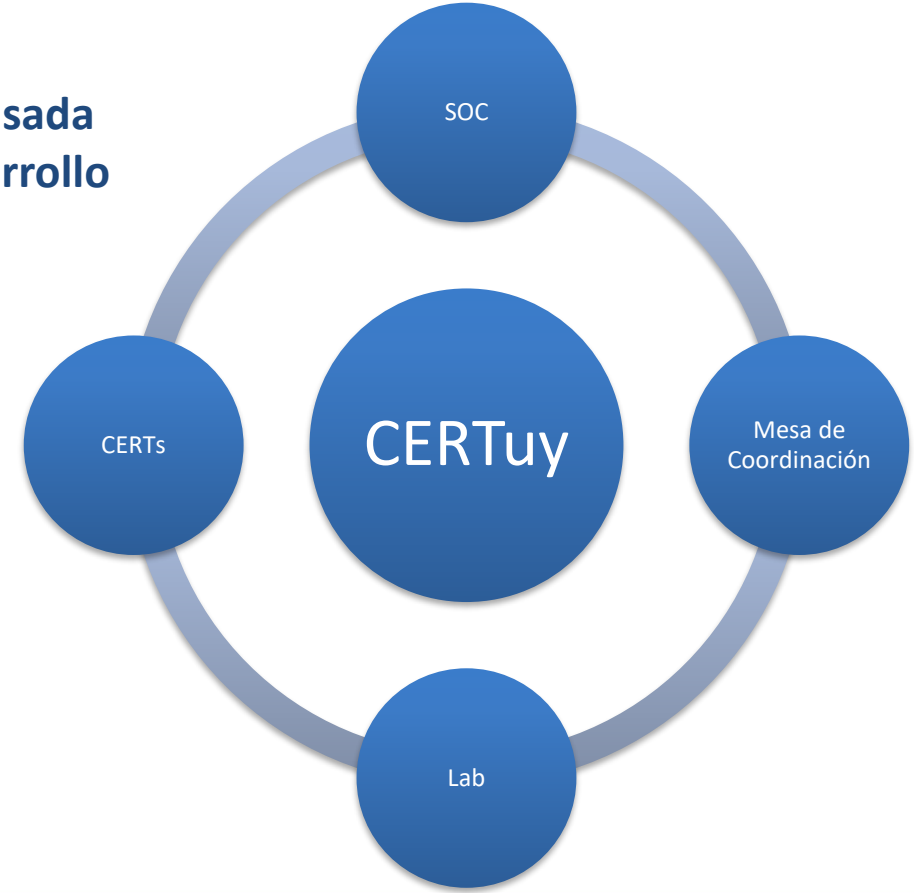
Gestión de riesgo y continuidad operativa

Privacidad y protección de datos personales.

Ecosistema de ciberseguridad	Centro Nacional de Operación de Ciberseguridad	Sistemas informáticos seguros en el sector privado	Mejorar el capacidades contra el cibercrimen
Gestión de riesgos y continuidad operativa	Marcos de Cyberseguridad	Requerimientos Mandatorios para Activos Críticos	Auditar modelos y cumplimiento de requerimientos
Universalizar la identificación electrónica	Ecosistema de identificación electrónica	Servicio de identificación móvil	Universalización de la identificación electrónica
Privacidad y protección de datos personales	Evolución del marco legal nacional	Buenas prácticas de privacidad desde el diseño	Incluir la PDP en la agenda pública y en la educación

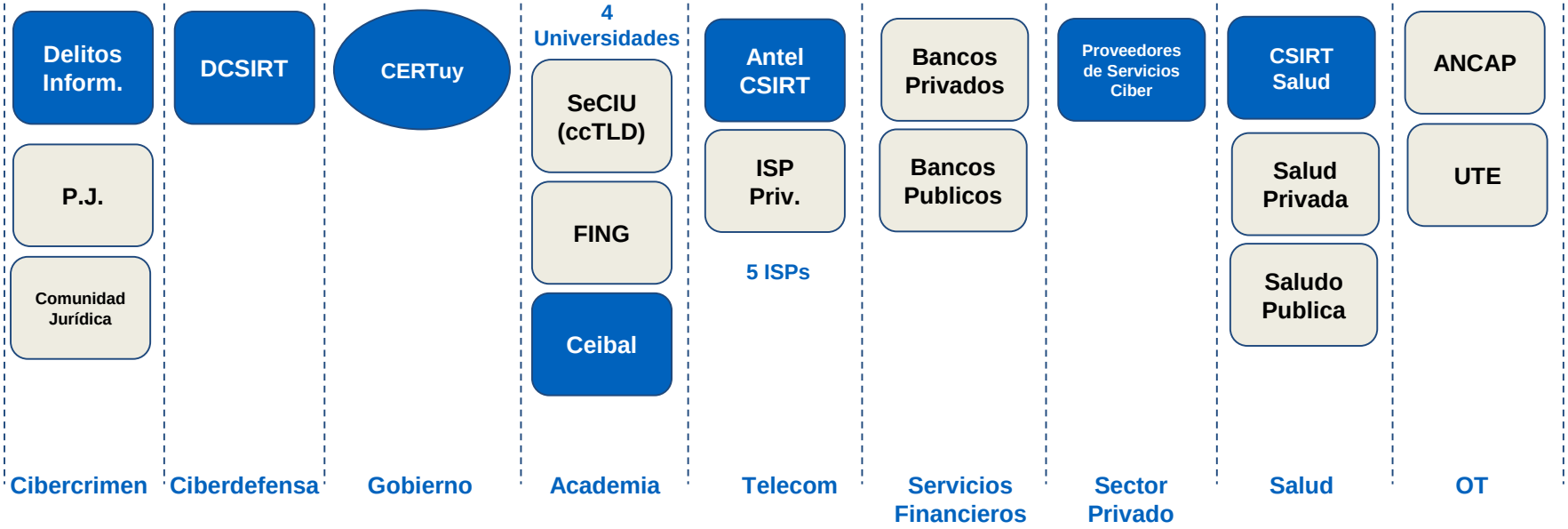
2016 - 2020

La estrategia de ciberseguridad está basada en la sinergia y el desarrollo de capacidades



Ecosistema de Ciberseguridad

AGESIC
(eID, CERTuy, SOC, Auditoría y Gestión)



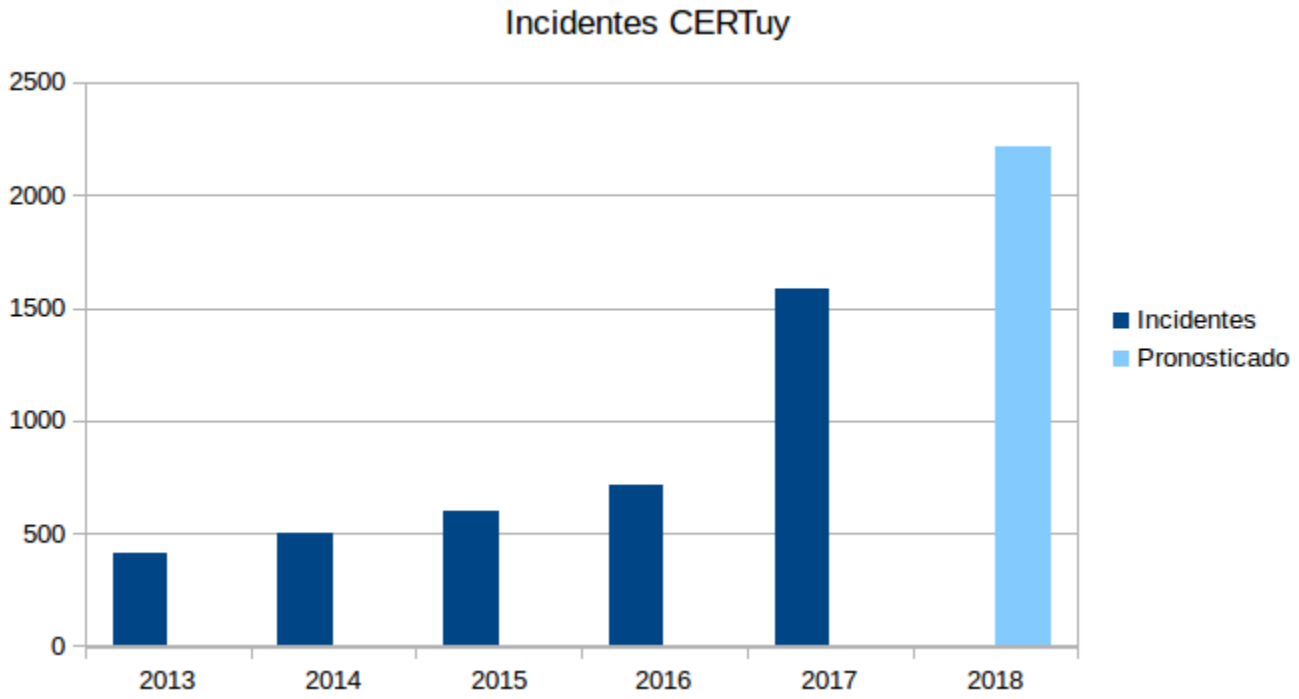

…Winter is coming...

Riesgo

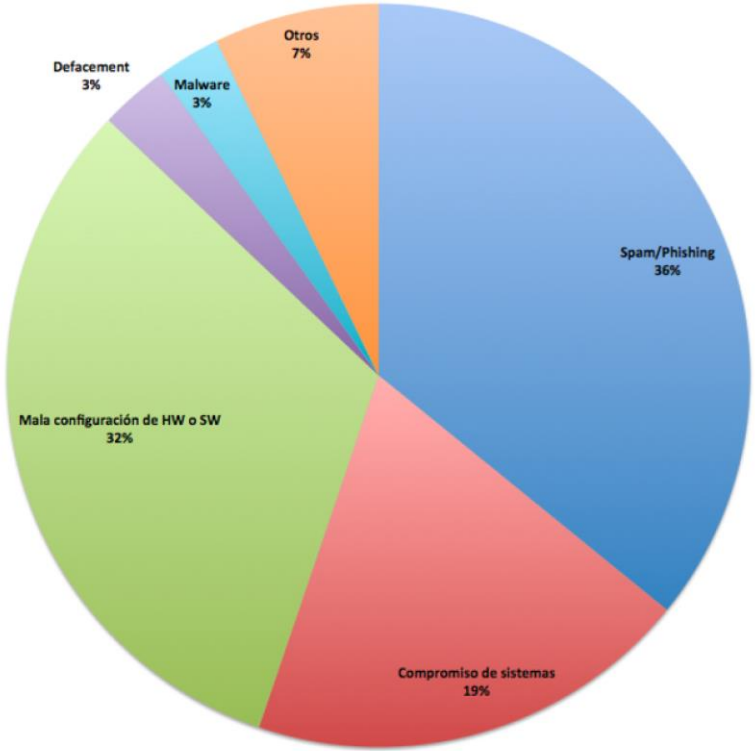

Vulnerabilidades
Tendencias
Nivel de amenaza
Probabilidad de ocurrencia
Estadísticas
Infraestructuras Envejecidas
Fronteras


Dependencia Tecnológica
Resiliencia
Diseños seguros
Impacto
Controles
Continuidad operativa
Políticas

Estadísticas CERTuy



Estadísticas CERTuy



- 36% - Spam/Phishing
- 32% - Mala configuración de HW o SW
- 19% - Compromiso de sistema
- 7% - Otros
- 3% - Malware
- 3% - Defacement

Los 3 pilares de la seguridad

Gestión y normativa

Establecer el marco de trabajo. Medir. Mejorar. Cumplimiento

Mejores Prácticas y controles

Minimizar los riesgos. Seguridad eficiente

Sensibilización

Generar conocimiento, entendimiento y cambio de hábitos.

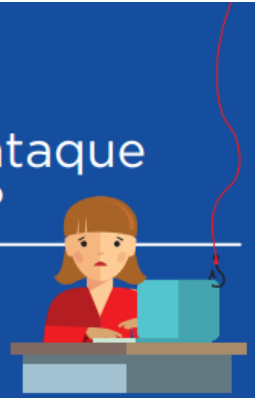
Uso seguro de contraseñas

Las contraseñas son las llaves de acceso a los sistemas que usamos (mail, red social, banca electrónica) y, por tanto, deben elegirse y protegerse de forma adecuada.

¿Cómo podés proteger tus cuentas?

- Elegí contraseñas que no contengan palabras relacionadas con el sitio utilizado o con características personales.
- Procurá tener diferentes contraseñas para cada servicio. De esta forma, si se comprometen los datos de una cuenta no se verán afectadas las demás.
- No accedas a tu cuenta bancaria o correo electrónico desde equipos en cibercafés o aeropuertos.
- Cambiá todas tus contraseñas regularmente; de esta forma, en caso de haber sido comprometidas, dejás sin acceso al atacante.
- Utilizá contraseñas complejas, es decir, de más de 8 caracteres, que contengan espacios, símbolos, números, mayúsculas y minúsculas.

¿Qué es un ataque de phishing?



El phishing es un tipo de ataque informático con el que se obtiene información personal o financiera de los usuarios como contraseñas, números de tarjetas de crédito o cuentas bancarias.

El ataque de phishing ocurre mediante correos electrónicos que le llegan al usuario y que imitan el formato, el lenguaje y la imagen de los mensajes emitidos por los bancos u otras instituciones. Estos mensajes engañosos siempre solicitan a los usuarios la confirmación de sus datos personales alegando problemas técnicos, cambios en las políticas de seguridad o fraude, entre otros.

¿Qué podés hacer para prevenir un ataque por Phishing?

→ Cuando accedas a tu banco en línea, evitá acceder a través de links, ingresá manualmente la dirección.

→ Antes de iniciar sesión para ingresar a tu cuenta bancaria, confirmá que la dirección web del banco sea la correcta y corroborá si en la barra del navegador aparece el candado que indica la autenticidad del sitio.

→ Tené presente que un banco nunca te solicitará información personal o confidencial por correo electrónico o por teléfono. En caso de recibir una notificación de este tipo, comunicate con tu banco de forma inmediata.

¿Qué es el ransomware?

El ransomware es el equivalente informático a un secuestro. Con este tipo de ataque se le bloquea al usuario el acceso a su información o equipos. De esta manera, solo el atacante puede recuperar esa información, por lo que exige un pago al usuario atacado a cambio de sus propios datos.

¿Qué podés hacer para estar preparado ante un ransomware?

Respaldá tu información de forma periódica, de modo que si sos víctima de ransomware puedas recuperarla sin pérdidas significativas.

No abras mensajes de correo electrónico no deseado, ni hagas clic en vínculos de sitios web sospechosos.

Evitá abrir archivos que provienen de fuentes poco fiables (mails con remitentes desconocidos, pendrives perdidos, entre otros).

Instalá un antivirus y mantenelo actualizado.

- Ley 18719 – Creación de la Dirección de seguridad
- Ley 18172 – Creación del CAHSI
- Ley 18362 – Creación del CERTuy
- Decreto 451/009 – Regulación del CERTuy
- Decreto 452/009 – Política de Seguridad de la Información
- Decreto 92/014 - Ciberseguridad
- Ley 18331: Protección de datos personales y acción de habeas data
- Ley 18381: Acceso a la información pública

Políticas de seguridad

Pol. Seguridad de la información

Pol. Acceso Remoto

Pol. Gestión de incidentes

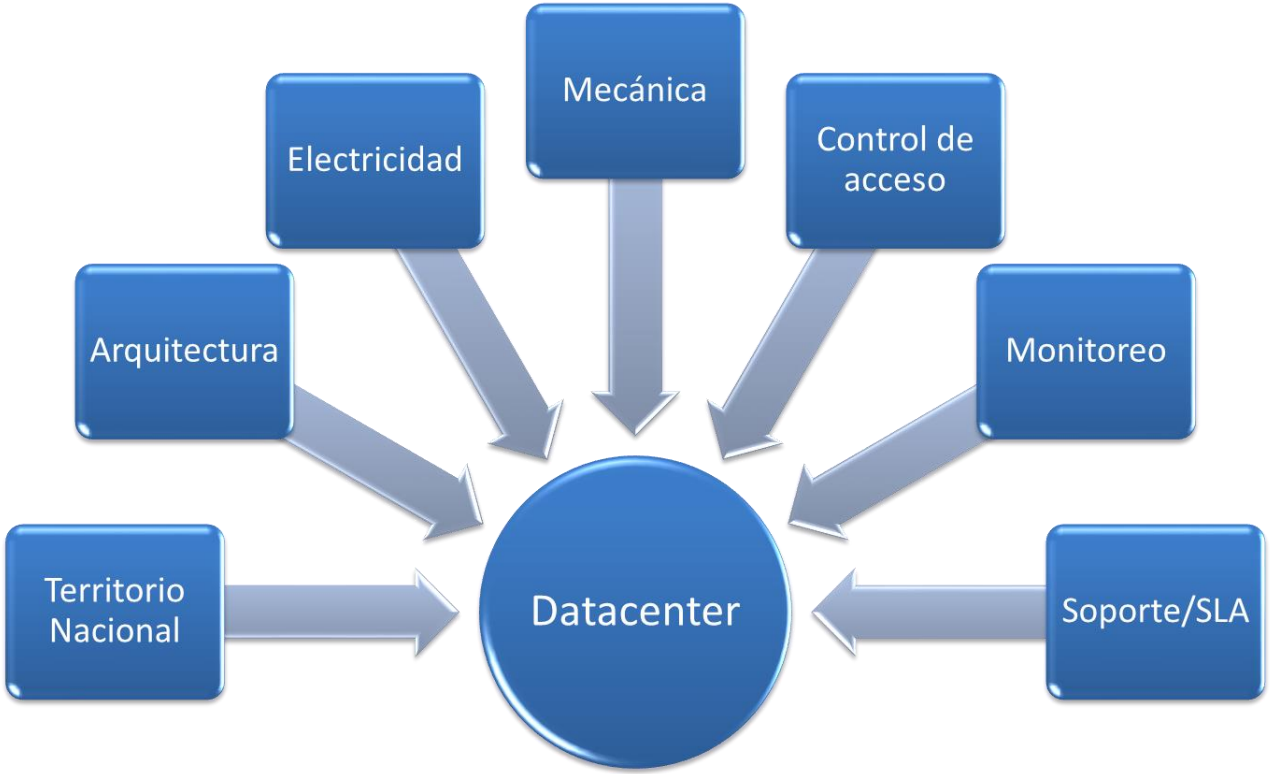
Pol. Respaldo de información

Pol. Protección contra software malicioso

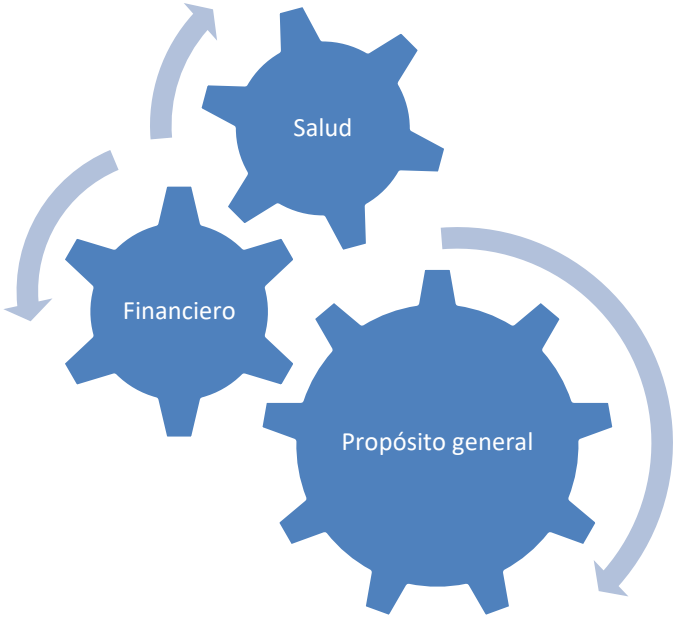
Pol. Gestión de usuarios y contraseñas

Pol. Control de acceso físico

Decreto 92/014 – Operaciones Seguras

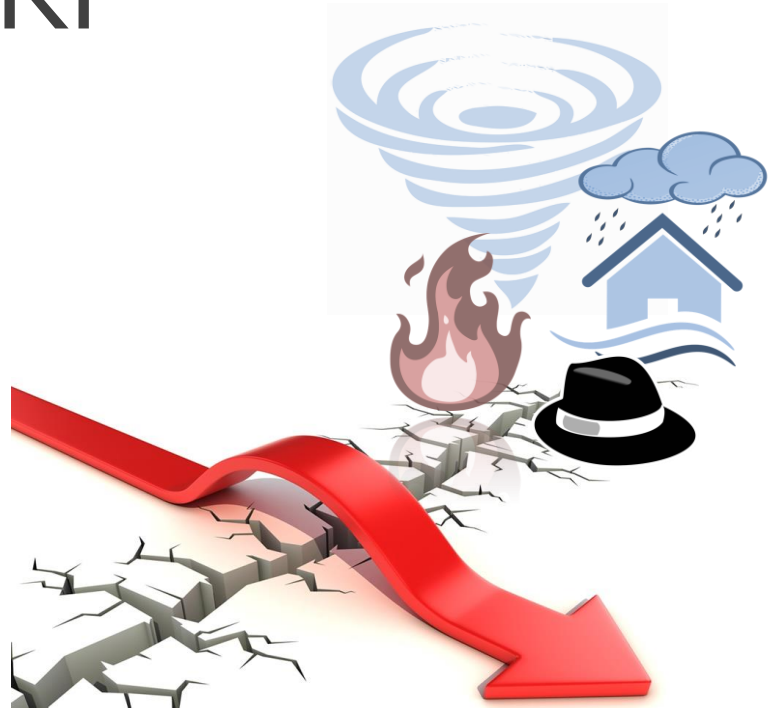


Marco de Ciberseguridad Uruguay

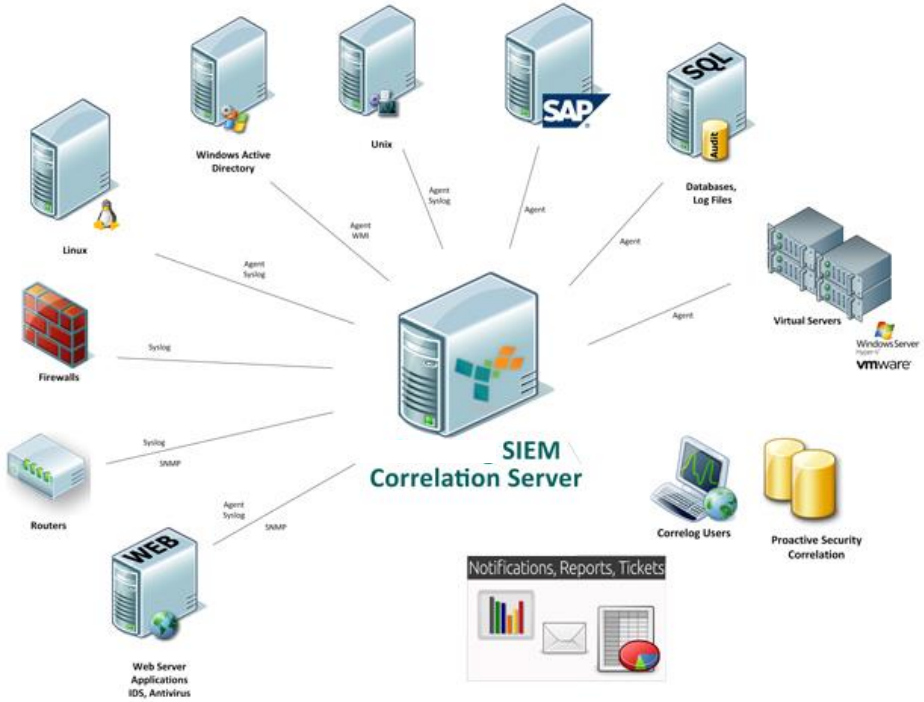


BUENAS PRÁCTICAS

BCP & DRP

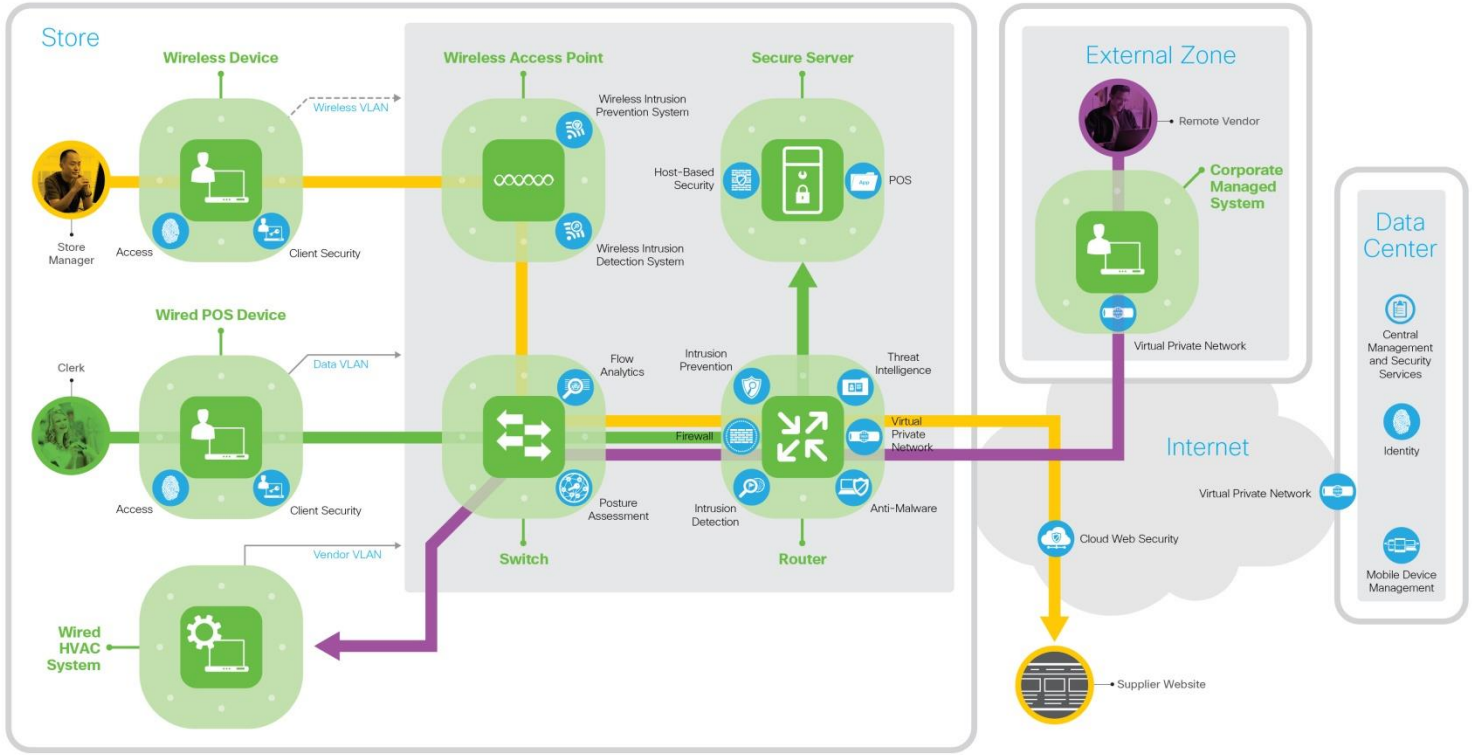


Concentración de trazas

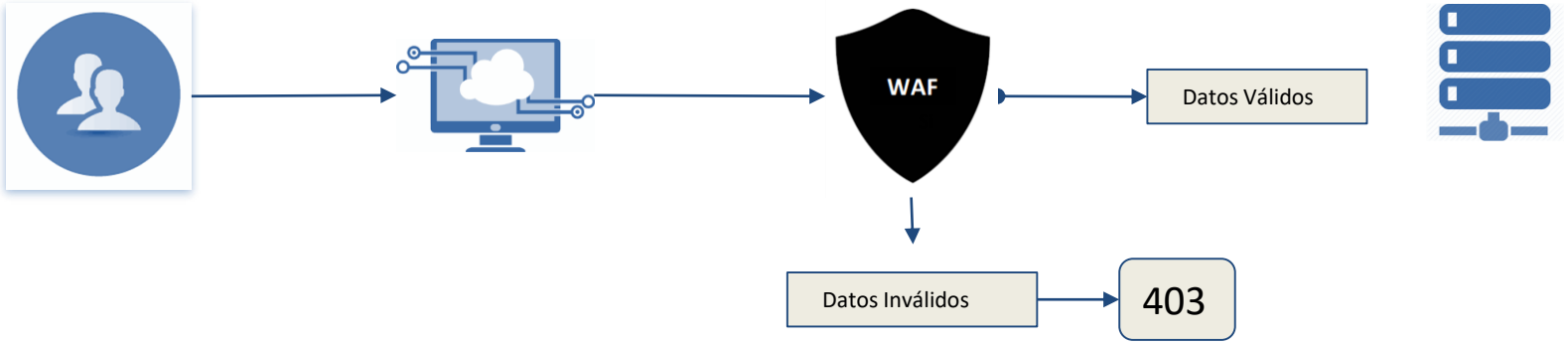



1600
1200
800
400
0
2013-07-05
2013-07-07
2013-07-09
2013-07-11

Diseño y arquitectura.



Web Applications Firewall (WAF)



Ethical Hacking

Pruebas de intrusión a los sistemas desde la perspectiva de un atacante, ejecutados por un equipo de expertos en seguridad ofensiva.

- **Alcance estipulado**
- **Plazos de pruebas autorizadas**

Informe de resultados con:

- **Recomendaciones.**
- **Matriz de riesgo asociada**
- **Evidencias y pruebas de regresión**

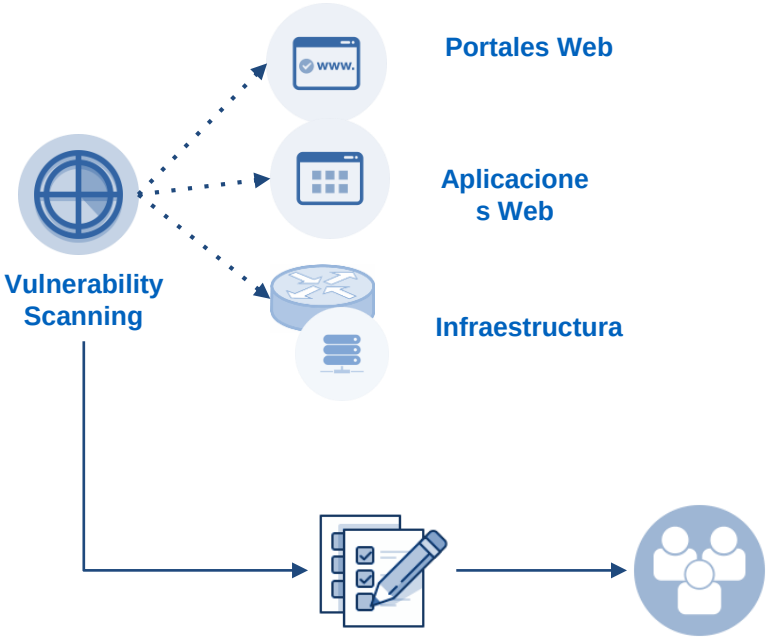
Ethical Hacker

Informe Ejecutivo + Informe Técnico

Gerencia

Administradores y Desarrolladores

Análisis de Vulnerabilidades



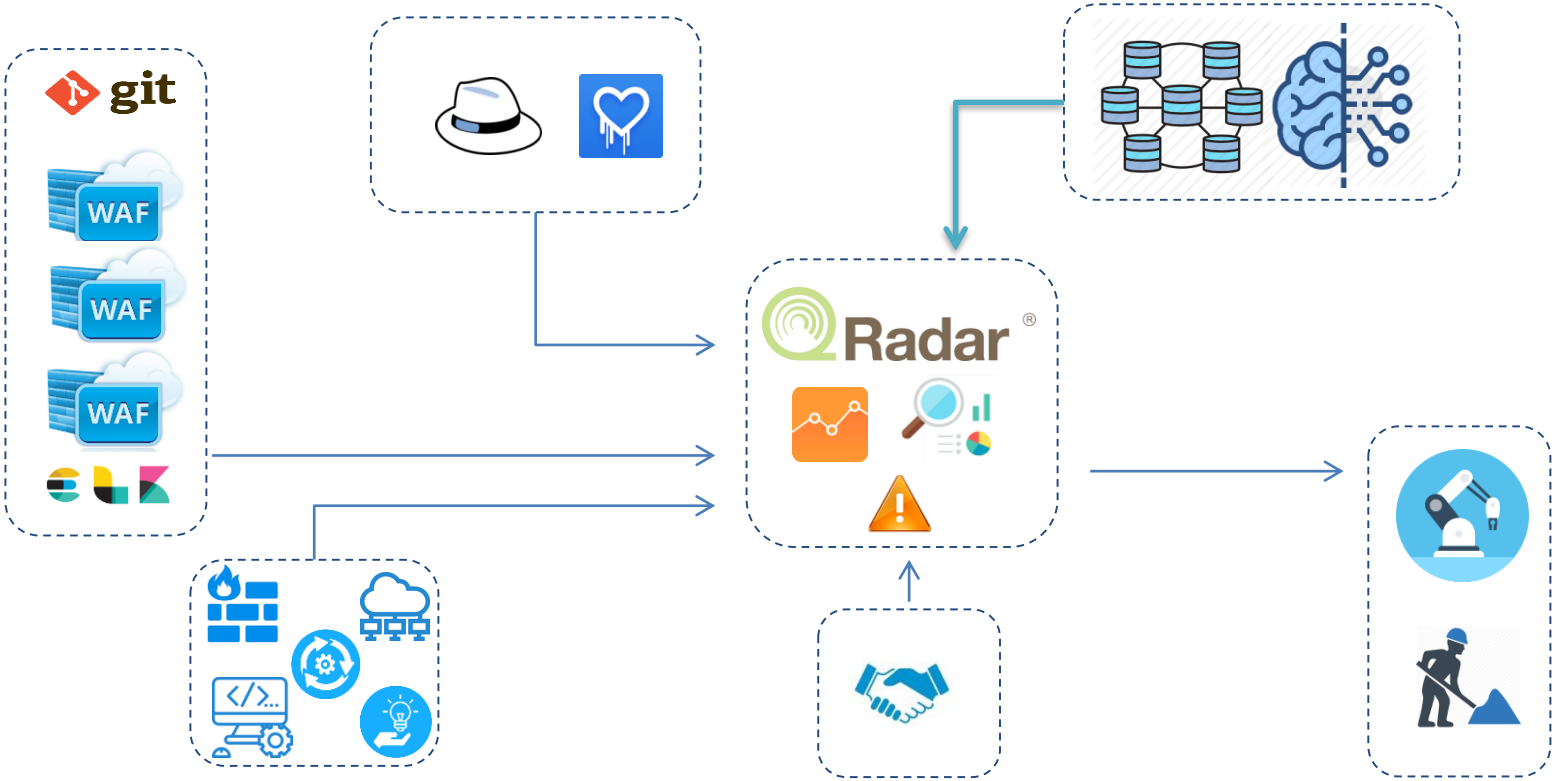
Escaneo automatizado por herramientas de análisis de vulnerabilidades; múltiples instancias anuales.

Poco entendimiento de negocio.

Informe genérico con clasificación de vulnerabilidades.

Cloud de Gobierno

Servicios de SOC… el futuro?




Gracias!!