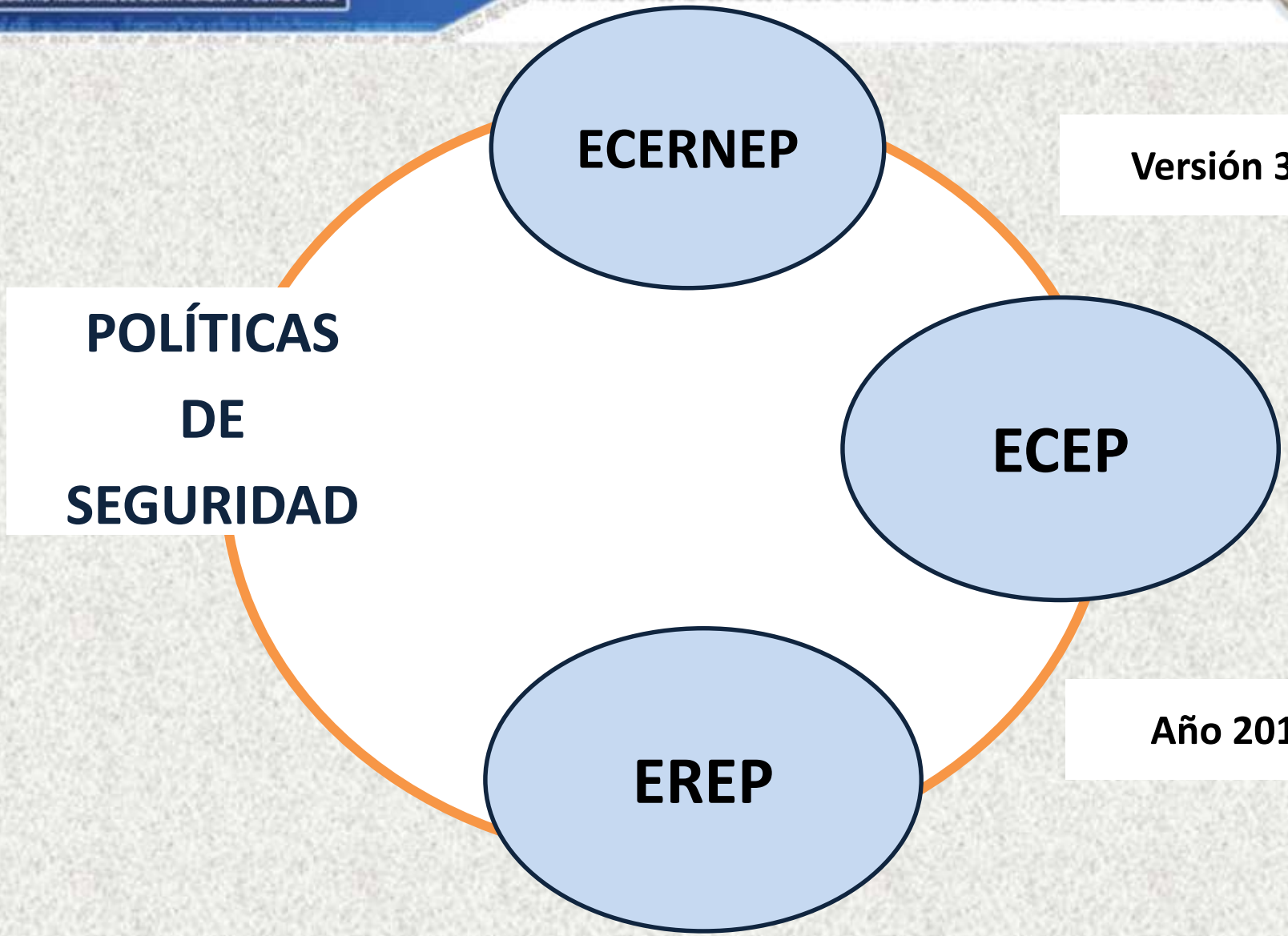
POLITICAS DE SEGURIDAD

ECERNEP – EREP - RENIEC

Ing. Andrés Martinez Panta
EREP-RENIEC (SGRD)



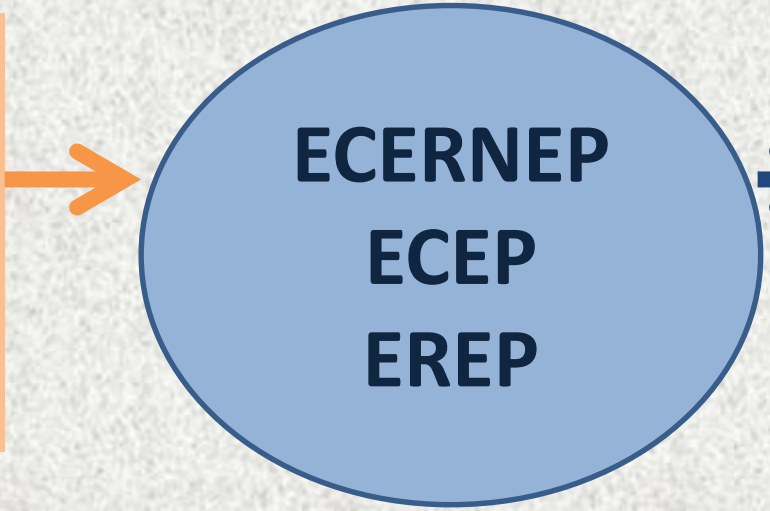
POLÍTICAS DE SEGURIDAD

Versión 3.0

Año 2013

OBJETIVOS

Establecer los lineamientos para la **Seguridad de la Información**



- **Disponibilidad**
- **Confidencialidad**
- **Integridad**

Establecer los lineamientos generales para detectar , reportar, evaluar y responder a los incidentes / vulnerabilidades de seguridad de la información identificado en el ámbito del proceso de certificación digital.

Activo

- Algo que tenga valor para la institución

Los equipos informáticos y mas aún la información almacenada en equipos informáticos

La documentación generada de los procesos que se realizan en la oficina

Activo

El personal y mas aún el conocimiento adquirido

La documentación de reuniones

Certificado Digital

Amenazas

- Un causa potencial de un incidente no deseado

Controles

- Herramienta de la gestión de riesgos, puede ser administrativa, técnica, gerencial o legal.

Contraseñas

Antivirus

Políticas

Vulnerabilidades

- Debilidades de seguridad asociadas con los activos de información

Sistema Operativo desactualizado

Antivirus desactualizado

Contraseñas débiles

Riesgo

- Potencial de que una amenaza dada explote las vulnerabilidades de un activo o activos , causando pérdida o daño.

Virus

Vulnerabilidad

Activo protegido con un antivirus desactualizado

Riesgo

Si el antivirus está desactualizado, el virus podría dañar la información

Incidencia de seguridad de la información

- Una o varios eventos inesperados y no deseados.

Virus

Vulnerabilidad

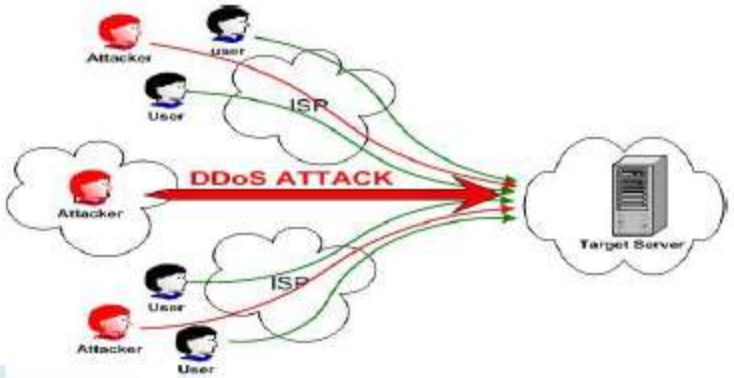
Activo protegido con un antivirus desactualizado

Incidencia

Con el antivirus desactualizado, el virus dañó la información

Tipos de incidentes

Deliberado	Accidental	Error
Acceso no autorizado	Fallas de hardware	Error de mantenimiento
Robo de información	Fallas de software	Error de usuario
Alteración de datos	Fallas de red	Error de diseño
Código malicioso	Fuga de agua	Error de configuración
Software ilegal		
Robo		
Mal uso de recursos		
Daños físicos		
Abuso de privilegios		



Gestión de riesgo

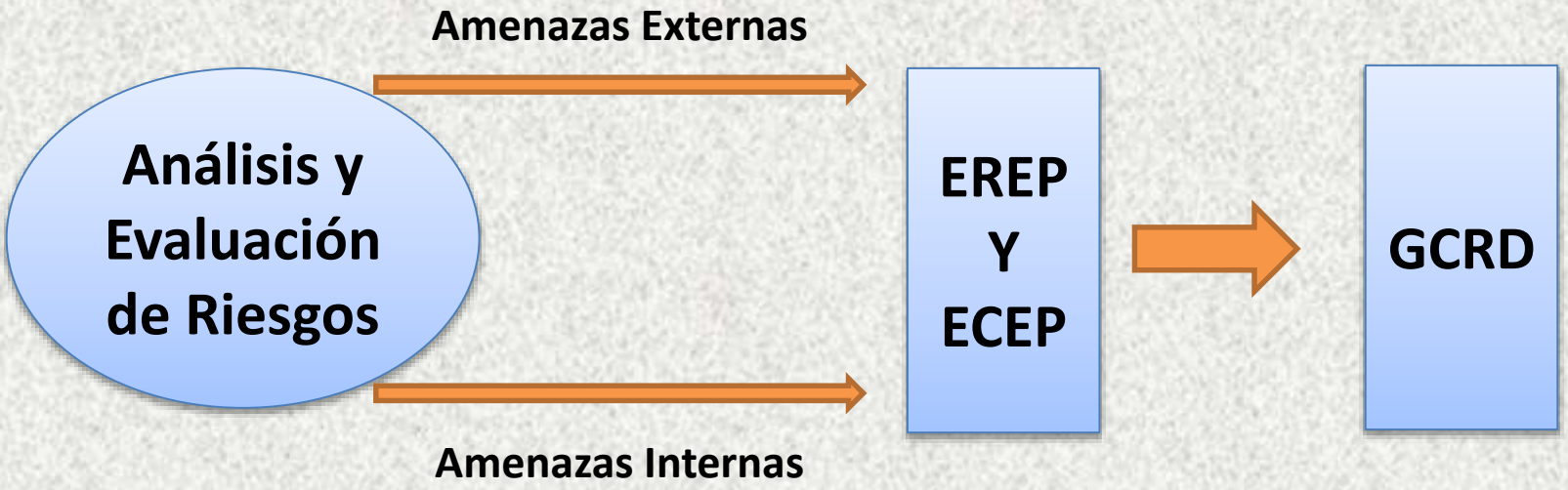
- Actividades coordinadas para dirigir y controlar una organización considerando el riesgo.
- Lo que se busca es mitigar los riesgos.

Alcances

- Evaluación de riesgos
- Control de accesos
- Seguridad de personal
- Seguridad física
- Seguridad de comunicaciones y redes
- Mantenimiento de equipos y su desecho
- Control de cambios y configuraciones
- Planificación de contingencias
- Respuesta a incidencias
- Auditorias y detección de intrusiones
- Medios de almacenamiento

Evaluación de Riesgos

Para cada proceso vital o crítico que se desarrolla en el ámbito de la EREP y ECEP se deberá efectuar:



Control de Accesos

El personal que reciba una cuenta de usuario de acceso deberá hacer uso adecuado de sus contraseñas de acceso, manteniendo la confidencialidad, no dejando sus estaciones de trabajo desatendidas solicitando su cambio de contraseña si tiene algún indicio de su vulnerabilidad.

Recomendaciones: seleccionar una contraseña con un nivel adecuado de complejidad.

Es responsabilidad del encargado o supervisor de cada órgano o unidad orgánica solictar en el menor tiempo posible la inactivacion de las cuentas de usuario cuando estos ya no presten servicios para la ECERNEP – ECEP – EREP o cuando el usuario o entidad externa ya no requiera del acceso.

Seguridad de Personal

- Antes del Empleo
  - Los perfiles de los puestos deberán ser definidos en base a las funciones que se van a desarrollar.
  - Cada una de las personas que prestan servicios en la ECERNEP, ECEP-RENIEC, EREP-RENIEC deben firmar un acuerdo de confidencialidad.

Seguridad de Personal

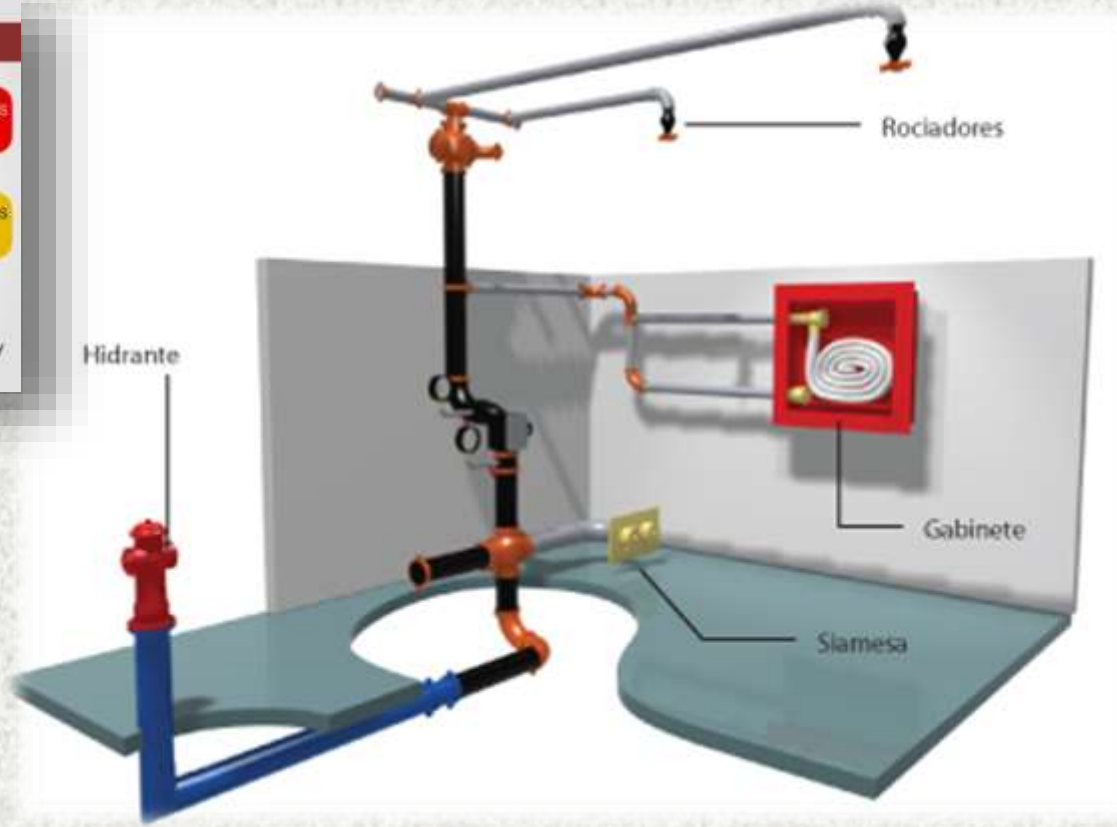
- Durante del Empleo
  - Toda persona que presta servicios en la ECERNEP, ECEP-RENIEC, EREP-RENIEC, recibirá charlas de inducción en materia de Seguridad de la Información.
  - Se deben desarrollar actividades de capacitación continua dirigidas a mantener actualizados los conocimientos del personal respecto al uso y reserva de la información.

Seguridad de Personal

- Finalización del Empleo
  - Todo cambio o finalización de funciones deberá realizarse de acuerdo a los procedimientos de RENIEC, incluyendo la entrega de bienes. De igual modo el supervisor deberá solicitar el retiro de accesos a la información o servicios de ECERNEP, ECEP-RENIEC, EREP-RENIEC.

Seguridad Física

Seguridad Física



Seguridad de Comunicaciones y Redes

Señal inalámbrica protegida con contraseña

Bloqueo de páginas

Seguridad de Comunicaciones y Redes

Datos viajan encriptados

Se protege de ataques externos

Mantenimiento de equipos

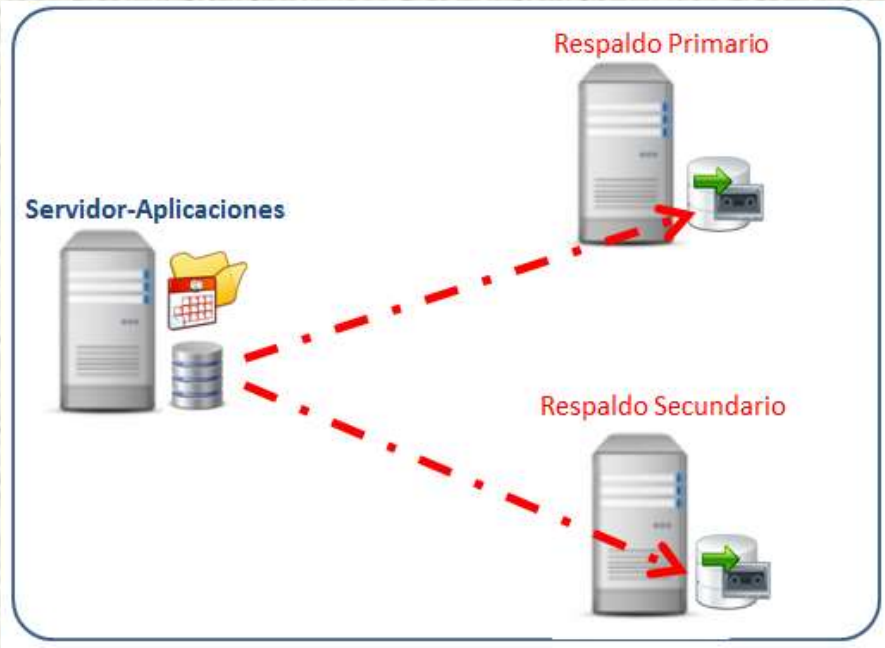
- Plan de mantenimiento preventivo.
- El reemplazo, manipulación y desecho, tanto del hardware y software se realizarán a los criterios establecidos por RENIEC.

Control de cambios y configuración

- Se ha dispuesto que todo cambio o modificación que se realice al sistema sea debidamente documentado, y de preferencia fuera del horario de atención a los clientes.

Planificación de contingencias

- Se implementará un plan de contingencias a nivel de servicios, que les permita reaccionar ante una posible interrupción en la actividades criticas del proceso de certificación digital.



Respuesta a incidentes

- Se deberá clasificar, comunicar y atender los incidentes de manera rápida, eficaz y sistemática, a fin de garantizar el restablecimiento del servicio afectado.
- Se deberá comunicar oportunamente al Oficial de Seguridad de Información o persona designada.

Auditorias y detección de intrusiones

- Se programarán como mínimo auditorias semestrales.
- Se deberán ejecutar pruebas periódicas de detección de intrusiones, así como la implementación de los respectivos controles.

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

FIN Y GRACIAS