OLACEFS

ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE
DE ENTIDADES FISCALIZADORAS SUPERIORES

CONTRALORÍA
GENERAL DE LA REPÚBLICA

XXV ASAMBLEA GENERAL OLACEFS

SANTIAGO DE QUERÉTARO, MÉXICO

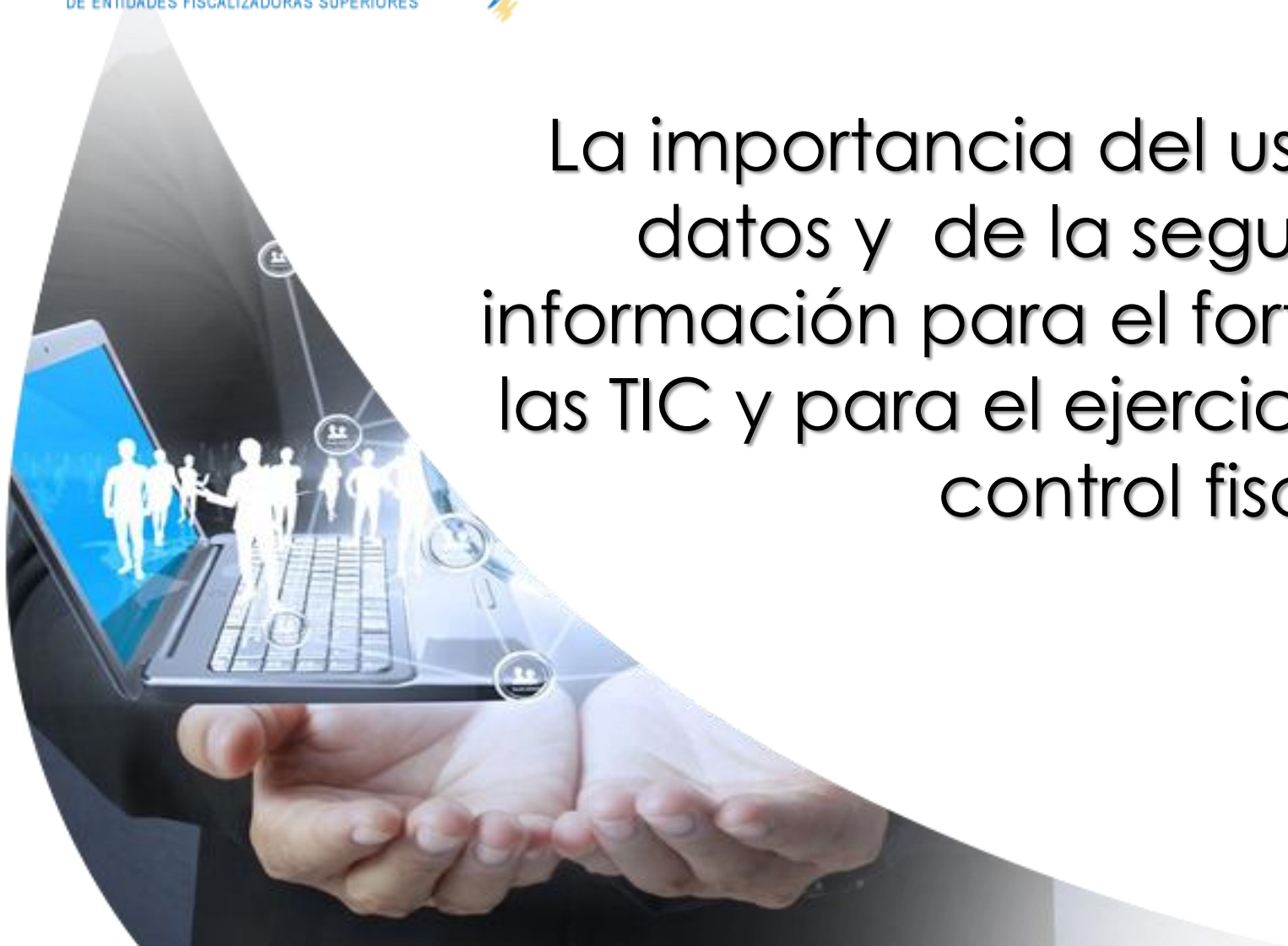
Adaptado de: Ramírez-Alujas y Dassen, 2012

Noviembre 23 al 27 de 2015

OLACEFS

ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE
DE ENTIDADES FISCALIZADORAS SUPERIORES

CONTRALORÍA
GENERAL DE LA REPÚBLICA



La importancia del uso de base de datos y de la seguridad de la información para el fortalecimiento de las TIC y para el ejercicio eficiente del control fiscal

Saber. Proporciona información sobre lo que esta haciendo, planes de acciones y fuertes datos.
Ello fomenta la rendición de cuentas

Tomar parte. Promueve el derecho de la ciudadanía a participar en el diseño, implementación y evaluación de las políticas públicas. Las entidades públicas se benefician de los conocimientos, ideas y experiencia de los ciudadanos

Contribuir. Compromete e implica a los ciudadanos y demás agentes sociales en el esfuerzo por trabajar conjuntamente para resolver los problemas nacionales

Tomado: curso estrategias para el Gobierno Abierto en las americas ed #1 (OEA/CLAD)

Adaptado de: Ramírez-Alujas y Dassen, 2012

Cuáles son los controles adecuados y necesarios que requieren las EFS para garantizar la seguridad de la información?

Revisión Marco Normativo ISO27000

↓

Aplicación y encuesta de seguridad informática

↓

Recopilación y Análisis de Resultados

OLACEFS
ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE DE ENTIDADES FISCALIZADORAS SUPERIORES

CONTRALORÍA GENERAL DE LA REPÚBLICA

SISTEMAS DE SEGURIDAD DE LA INFORMACION (SGSI)

Revisión Marco Normativo ISO27000

- 27001: Requisitos SGSI
- 27002: Buenas prácticas para la gestión de seguridad (objetivos de control y medidas a tomar)

Aplicación Encuesta Seguridad Informática

ENCUESTA – DIAGNOSTICO

1. Buenas prácticas y herramientas con que cuentan las EFS para garantizar la seguridad de la información.
2. Mecanismos de seguridad empleados en el intercambio de información.
3. Existencia o proceso de conformación de equipos de respuesta a incidentes de seguridad informática y la implementación del SGSI.

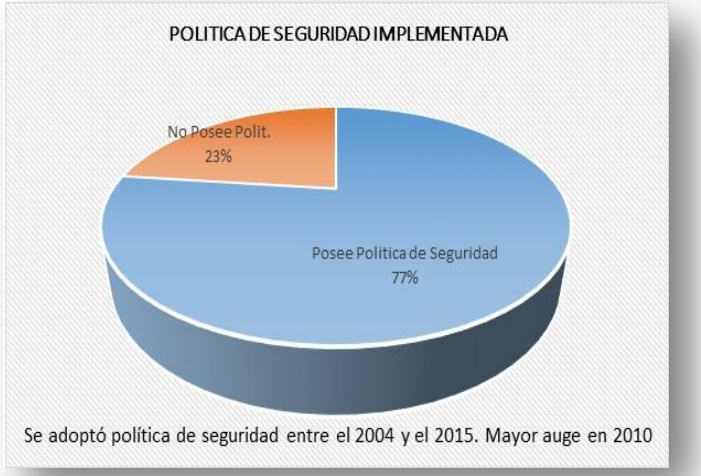
1

BUENAS PRACTICAS Y HERRAMIENTAS PARA LA SEGURIDAD DE LA INFORMACION

BUENAS PRACTICAS PARA LA SEGURIDAD DE LA INFORMACION

Se debe buscar un enfoque de seguridad integrado el cual busca ser **predictivo** y proteger de manera **proactiva** de cualquier incidente de seguridad.

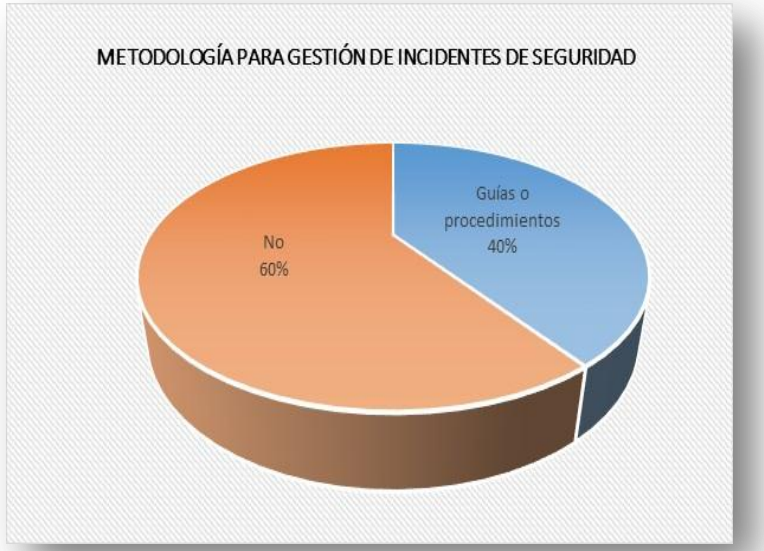
Requiere compromiso de la alta gerencia para generar estrategias y políticas y socializarlas a los empleados, terceras partes y clientes.

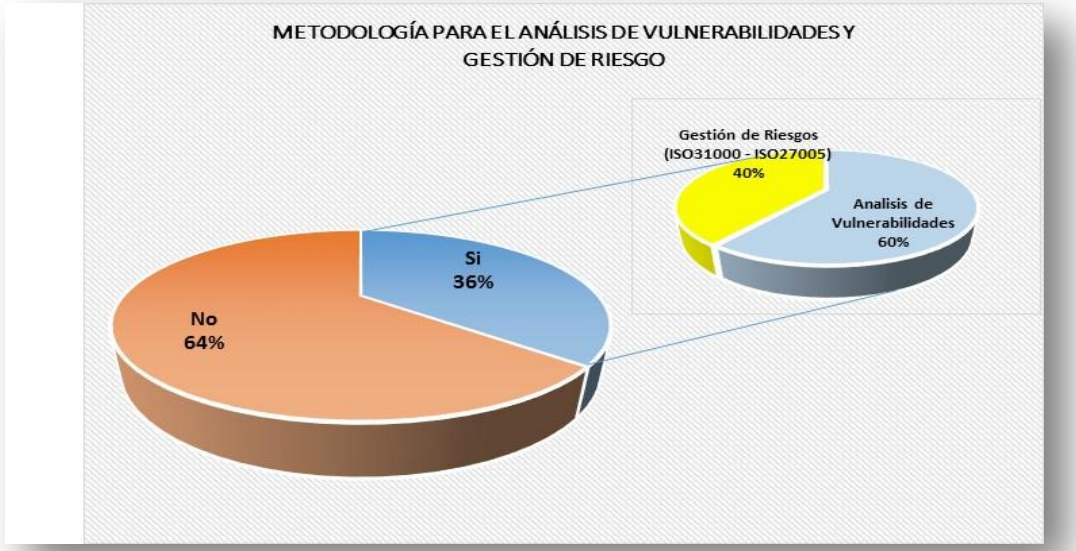


BUENAS PRACTICAS PARA LA SEGURIDAD DE LA INFORMACION

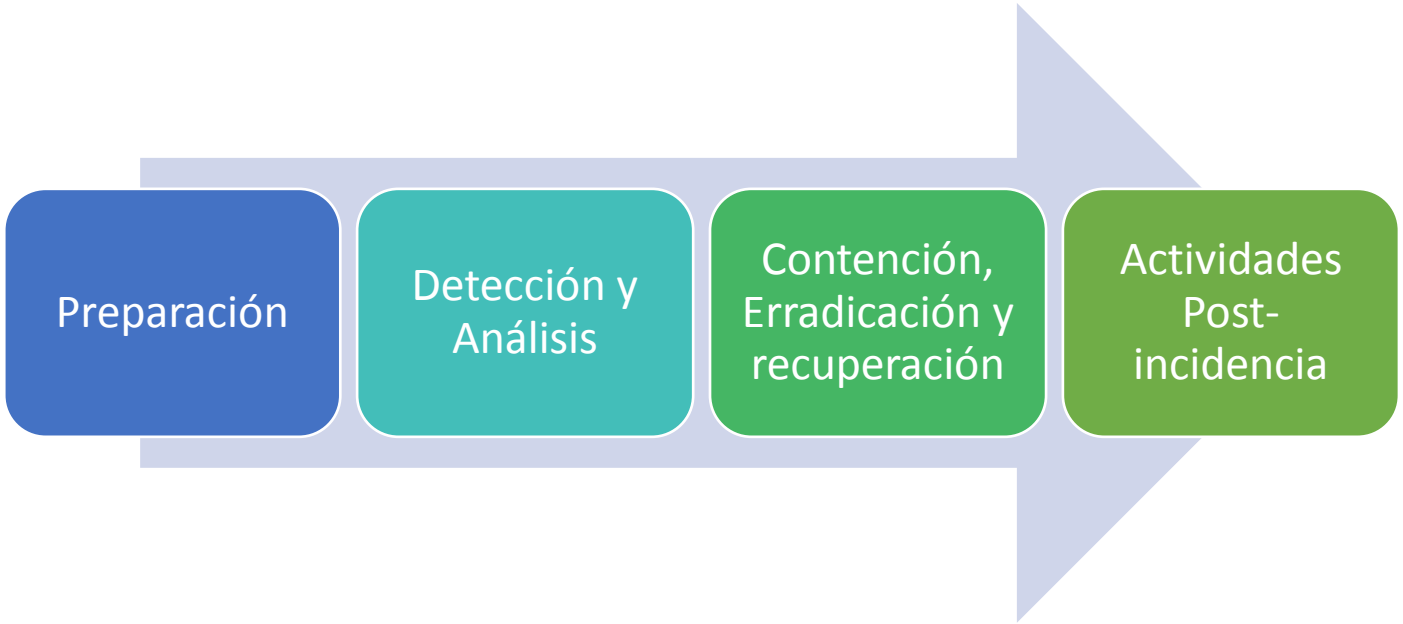
Se recomiendan metodologías para **gestión de incidentes**, análisis de vulnerabilidades y gestión de riesgos.

Falta avanzar en la aplicación de metodologías que incluyan planes y auditorias





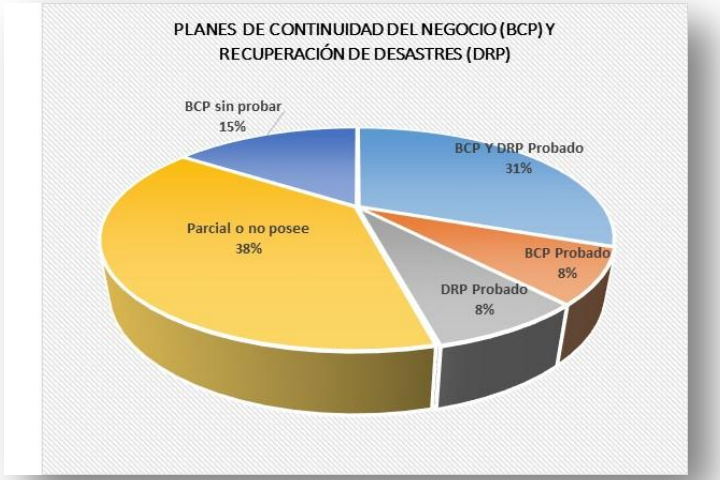
GESTION DE INCIDENTES: Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo se considera un "incidente" el cual debe ser gestionado con el propósito de tener control de los procesos, mejorar el uso de los recursos y determinar si genera o no riesgo para la operación.

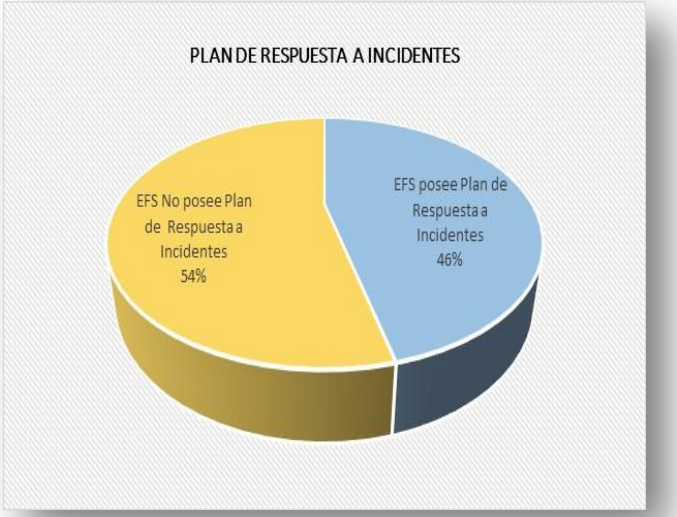


BUENAS PRACTICAS PARA LA SEGURIDAD DE LA INFORMACION

Se debe contar con un plan de **continuidad de negocio** y planes de **recuperación de desastres.**

Se deben establecer procedimientos específicos que respondan a interrupciones del servicio para proteger funciones criticas del negocio (sistemas de información y personas).
Realizar pruebas de efectividad de los planes.





CONTINUIDAD DE NEGOCIO : Proceso en el cual se identifican impactos potenciales que amenazan la continuidad de actividades, proveyendo un marco para construcción de resiliencia y capacidad de respuesta efectiva ante disrupciones.

- Diseñar una estrategia de continuidad de servicios de TI
- Realizar un análisis de los recursos críticos de TI
- Mantener actualizado el plan a través de procedimientos de control de cambio
- Elaborar pruebas de continuidad
- Capacitar a los responsables en el el plan de continuidad y análisis de impacto de negocio

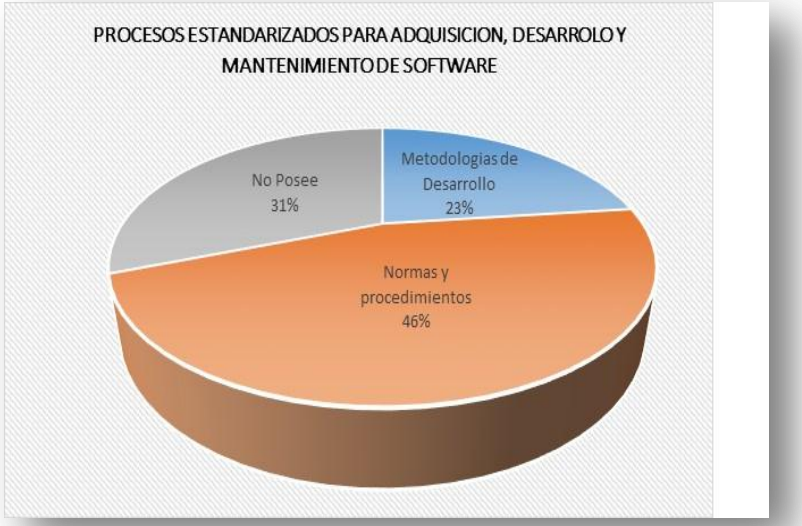
OLACEFS
ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE DE ENTIDADES FISCALIZADORAS SUPERIORES

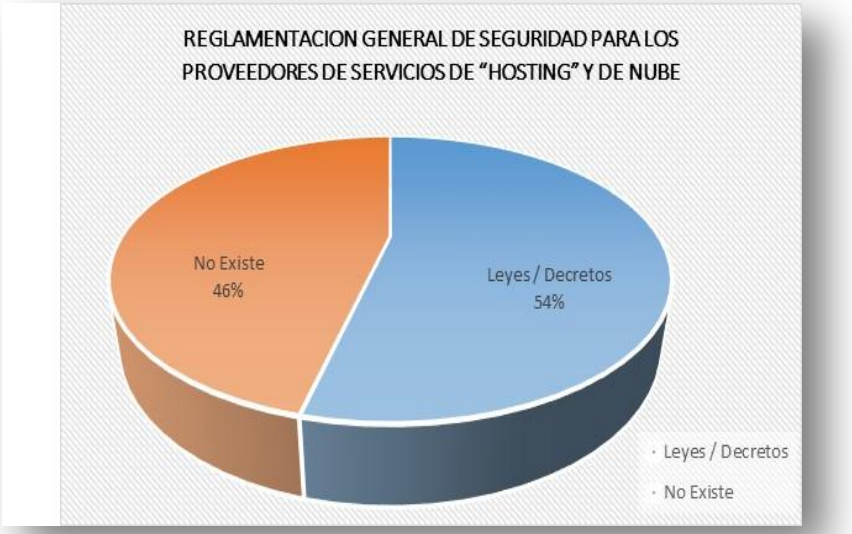
CONTRALORÍA GENERAL DE LA REPÚBLICA

HERRAMIENTAS PARA LA SEGURIDAD DE LA INFORMACION

Asegurar que en la adquisición y desarrollo de sistemas de información se incluyan **controles de seguridad y validación de datos, se definan métodos de protección de información crítica o sensible** y se documenten procedimientos y normas que apliquen en el ciclo de vida de los aplicativos y en la infraestructura de apoyo.

Se esta avanzando. Se están resolviendo aspectos de seguridad en la nube.





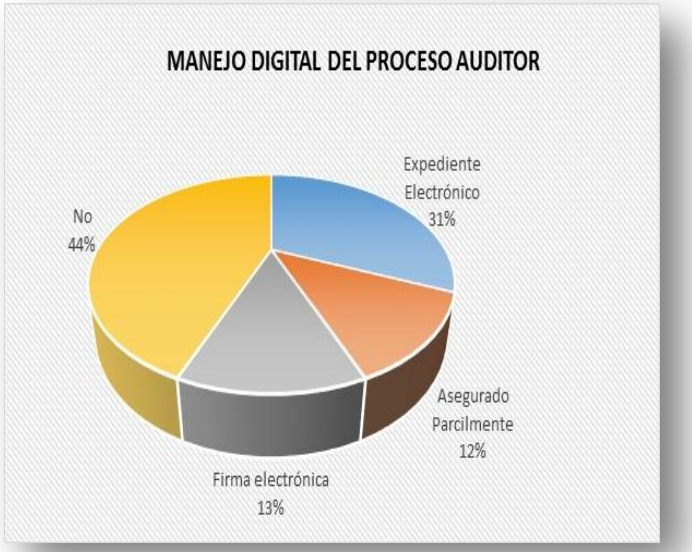
OLACEFS
ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE DE ENTIDADES FISCALIZADORAS SUPERIORES

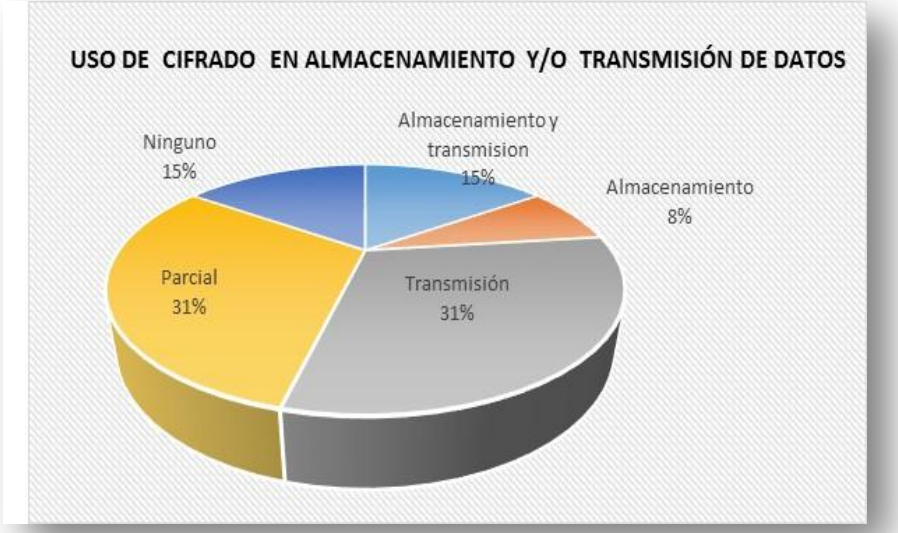
CONTRALORÍA GENERAL DE LA REPÚBLICA

HERRAMIENTAS PARA LA SEGURIDAD DE LA INFORMACION

Uso de **sistemas y técnicas criptográficas** para la protección de la información con base en el análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de la confidencialidad e integridad de la información.

Existe un potencial para explotar herramientas disponibles en el mercado





2

MECANISMOS DE SEGURIDAD EMPLEADOS EN EL INTERCAMBIO DE INFORMACIÓN.

OLACEFS
ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE DE ENTIDADES FISCALIZADORAS SUPERIORES

CONTRALORÍA GENERAL DE LA REPÚBLICA

MECANISMOS DE INTERCAMBIO DE INFORMACION

El 92% de las EFS colaboradoras realiza intercambio de información a través de redes de datos, web institucional y en casos puntuales a través de redes privada virtuales -VPN.

Las **medidas de prevención** usadas para asegurar la información no son muy claras, por ello se agruparon en tres categorías:

- 7 % : políticas de seguridad
- 52% : infraestructura de seguridad perimetral (firewall de red, anti spam)
- 41% : Monitoreo (antivirus, monitoreo de aplicaciones, y BD, correlación de eventos)

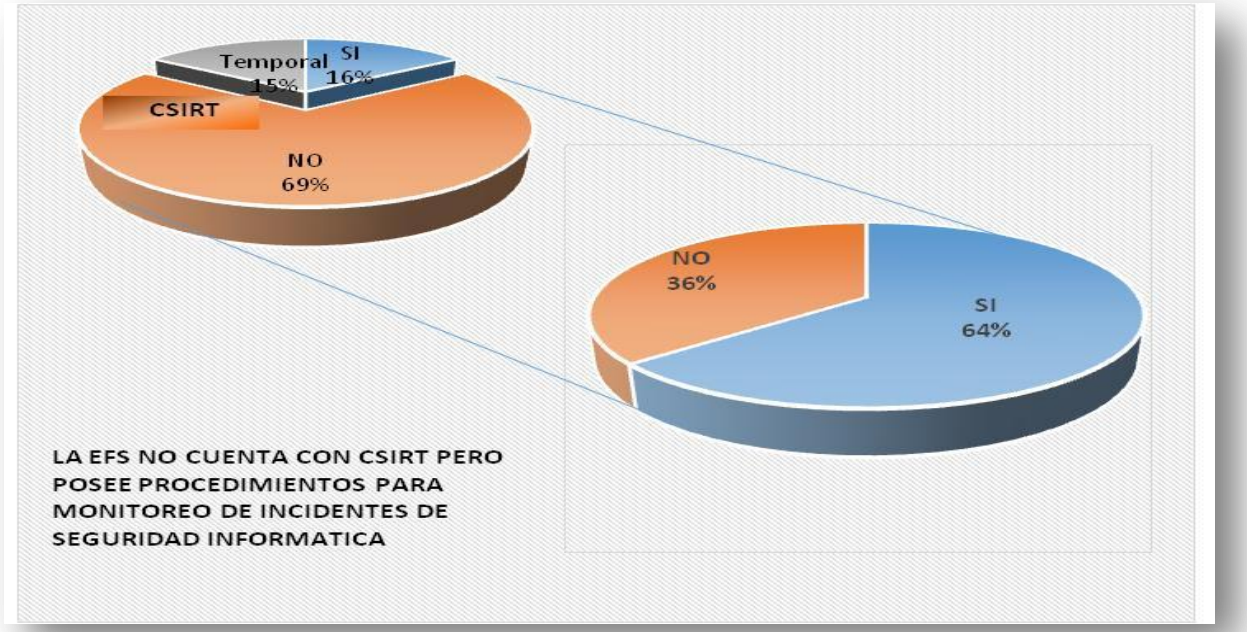
3

GRUPOS DE RESPUESTA A INCIDENTES

GRUPOS DE RESPUESTA A INCIDENTES

Se debe contar con personal especializado en seguridad informática

No hay grupos formales pero si el establecimiento de procedimientos de seguridad



GRUPOS DE RESPUESTA A INCIDENTES: Son equipos de trabajo especializados que realizan respuesta de manera centralizada a incidentes de seguridad.

CSIRT – Computer Security Information Response Teams

CERT – Computer Emergency Response Team

- Generación de Alertas y advertencias
- Gestión de incidentes
- Gestión de vulnerabilidades
- Observatorio Tecnológico
- Configuración y mantenimiento de herramientas
- Servicios de Detección de Intrusos
- Gestión de calidad
- Entrenamiento y Comunicaciones

OLACEFS
ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE DE ENTIDADES FISCALIZADORAS SUPERIORES

CONTRALORÍA GENERAL DE LA REPÚBLICA

RESULTADOS

Revisión Marco Normativo ISO27000

↓

Aplicación Encuesta Seguridad Informática

↓

Recopilación y Análisis de Resultados

- Buenas prácticas :
  - Compromiso de la alta gerencia
  - Gestión de Incidencias
  - Planes de Continuidad de Negocio
- Mecanismos de Intercambio de Información
  - Políticas de seguridad
  - Infraestructura de seguridad perimetral
  - Monitoreo
- Equipos de respuesta a incidentes

AGRADECIMIENTO

La Contraloría General de la República de Colombia, agradece la contribución realizada por los siguientes miembros de la Organización, que hicieron sus aportes de forma oportuna realizar el análisis del tema técnico para esta Asamblea:

1. *Controlaría General de la República de Cuba*
2. *Auditoria Superior de la Federación de México*
3. *Contraloría General de la República de Nicaragua*
4. *Contraloría General de la República Bolivariana de Venezuela*
5. *Contraloría General de la República de Chile*
6. *Auditoría General de la Nación de Argentina*
7. *Controlaría General de la República de Panamá*
8. *Cámara de Cuentas de la República Dominicana*
9. *Tribunal Superior de Cuentas de la República de Honduras*
10. *Oficia del Contralor del Estado Libre Asociado de Puerto Rico*
11. *Contraloría General de la República Perú*
12. *Contraloría General de la República de Costa Rica*
13. *Contraloría General de la República de Colombia*

Edgardo José Maya Villazón

OLACEFS

ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE
DE ENTIDADES FISCALIZADORAS SUPERIORES

CONTRALORÍA
GENERAL DE LA REPÚBLICA

Gracias