Taller:
Seguridad Digital (Normas Peruanas)

Mas allá de la Seguridad Digital….
SEGURIDAD DE LA INFORMACIÓN

Carlos Trigo Pérez

Sesión 4

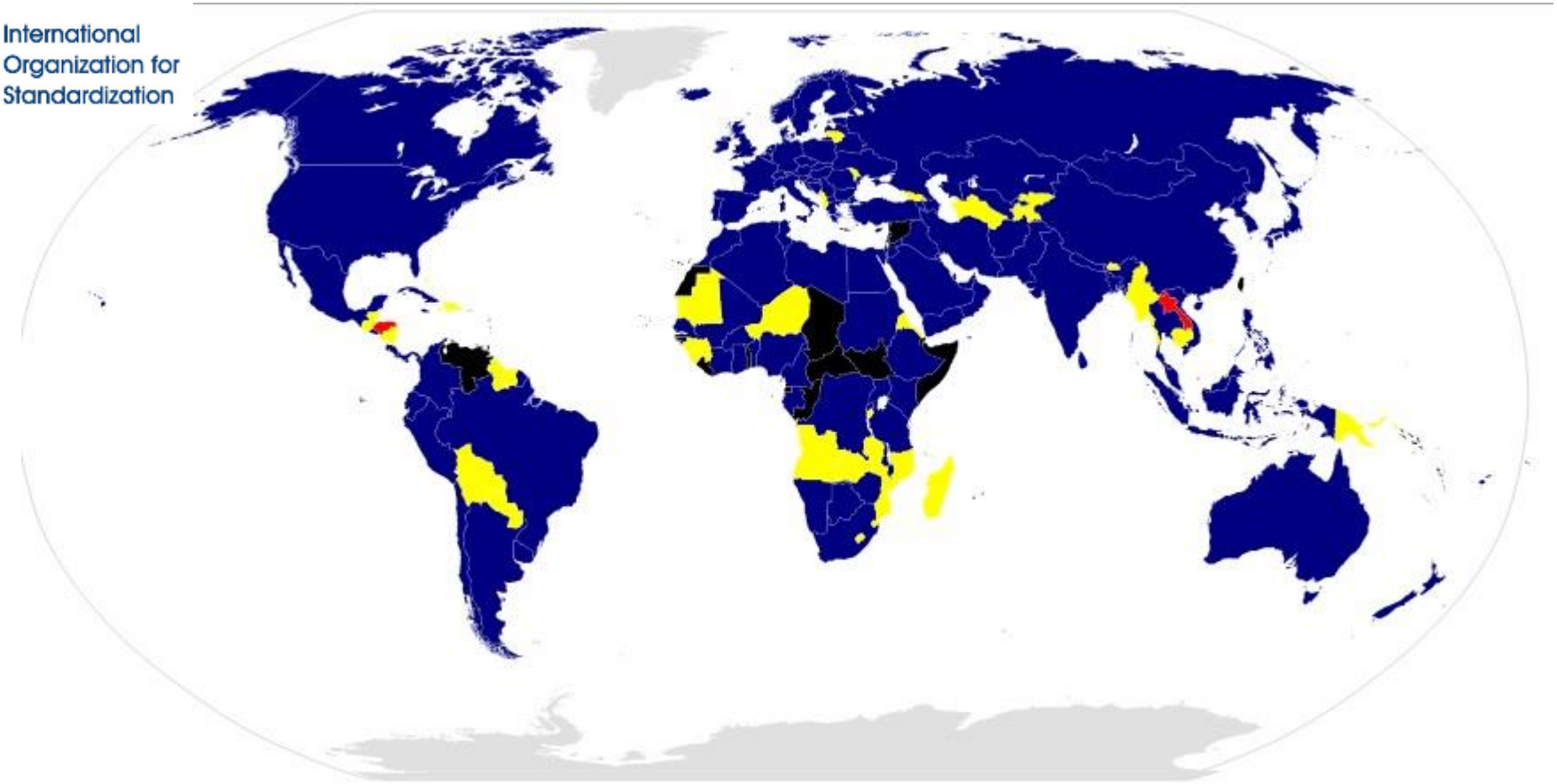
Agenda

- La norma ISO 27001, Controles y Política de seguridad
- Taller 4

Gestión de la Seguridad de la Información

La Norma ISO 27001

ISO International Organization for Standardization



- Países miembro de ISO con derecho a voto
- Miembros corresponsales (países sin un cuerpo nacional de estandarización).
- Miembros subscriptores (países con pequeñas economías)
- Países no-miembros con códigos

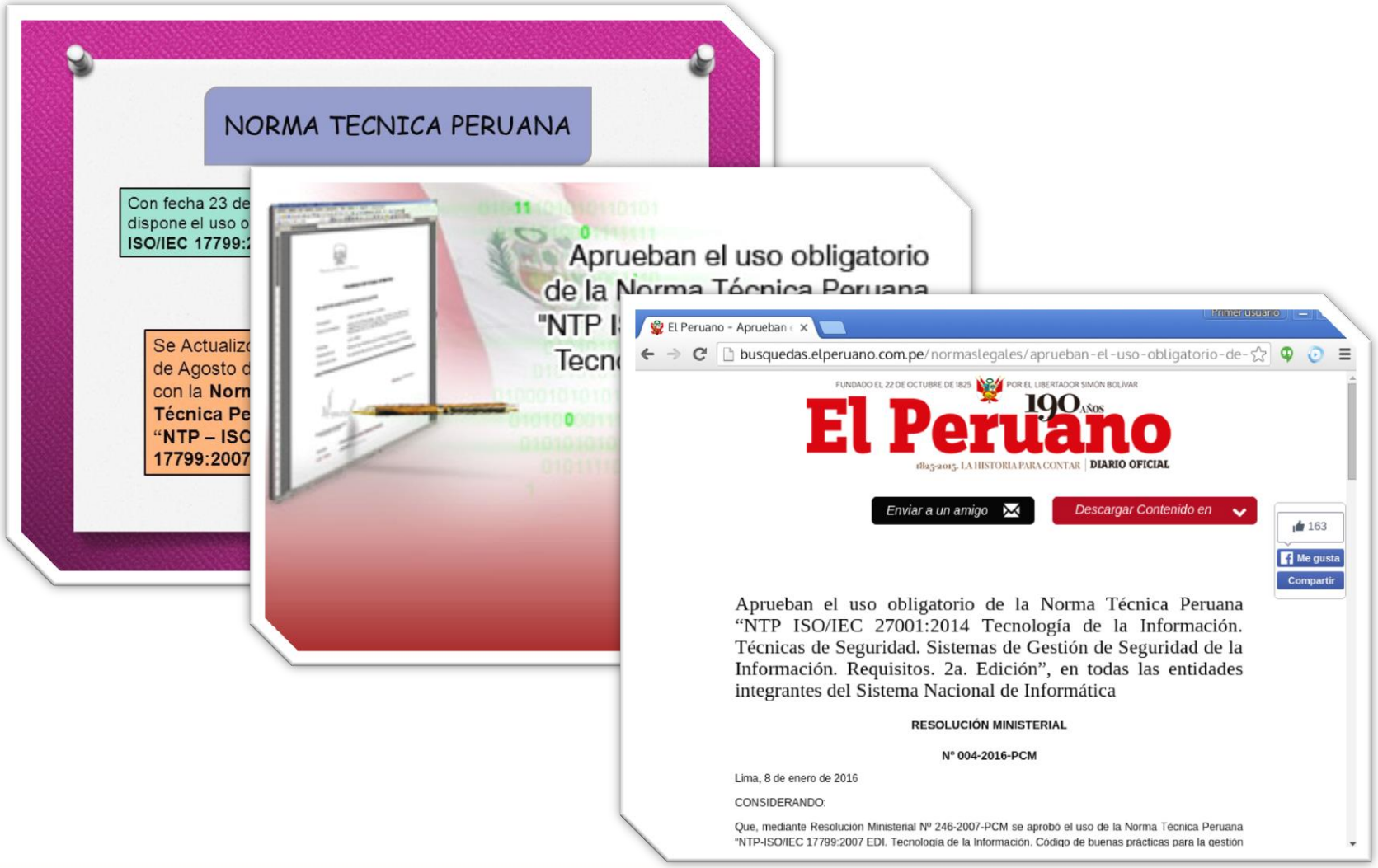
¿… Y en el Perú?

COMISIÓN DE REGLAMENTOS TÉCNICOS Y COMERCIALES

COMITÉ TÉCNICO DE NORMALIZACIÓN DE CODIFICACIÓN E INTERCAMBIO ELECTRÓNICO DE DATOS

LA CONTRALORÍA GENERAL DE LA REPÚBLICA
Deloitte & Touche
NSF INASSA
DROKASA PERU
GS1 Peru
DMS
E.WONG
ASSENDA UNA EMPRESA CARVAJAL
ITICSec
Oficina Nacional de Gobierno Electrónico e Informática Servicios ONGEI
ßzimprove
SUNAT
ET LUX IN TENEBRIS LUCET MCMXVII
PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Indecopi

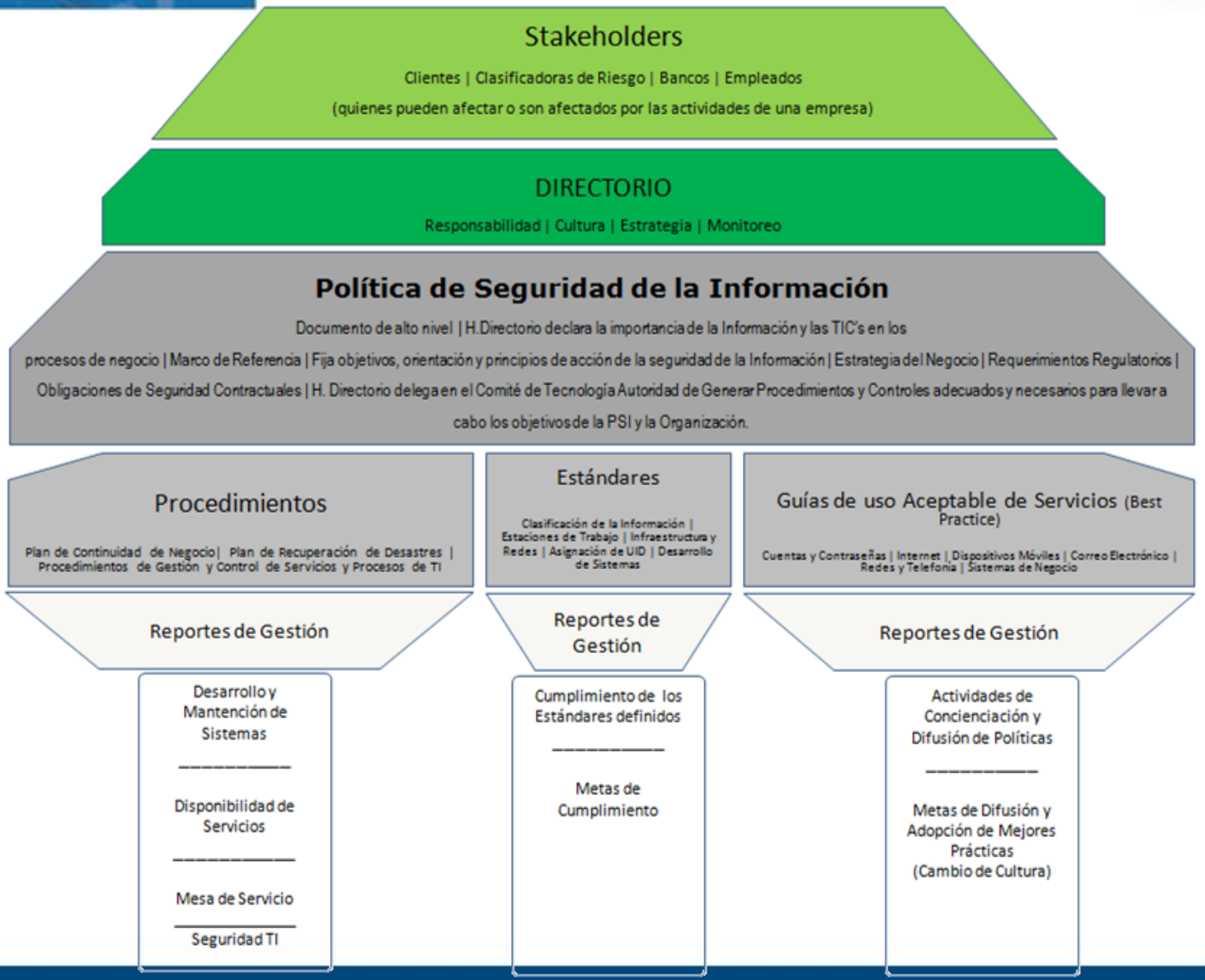
¿... Y en el Perú?


NORMA TECNICA PERUANA
Con fecha 23 de
dispone el uso o
ISO/IEC 17799:
Se Actualiz
de Agosto d
con la Norm
Técnica Pe
"NTP – ISO
17799:2007
Aprueban el uso obligatorio
de la Norma Técnica Peruana
"NTP I
Tecn
busquedas.elperuano.com.pe/normaslegales/aprueban-el-uso-obligatorio-de-
FUNDADO EL 22 DE OCTUBRE DE 1825 POR EL LIBERTADOR SIMÓN BOLÍVAR
El Peruano
190 AÑOS
1825-2015. LA HISTORIA PARA CONTAR | DIARIO OFICIAL
Enviar a un amigo
Descargar Contenido en
163
Me gusta
Compartir
Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática
RESOLUCIÓN MINISTERIAL
Nº 004-2016-PCM
Lima, 8 de enero de 2016
CONSIDERANDO:
Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión

Implementando la Norma NTP ISO/IEC 27001:2014

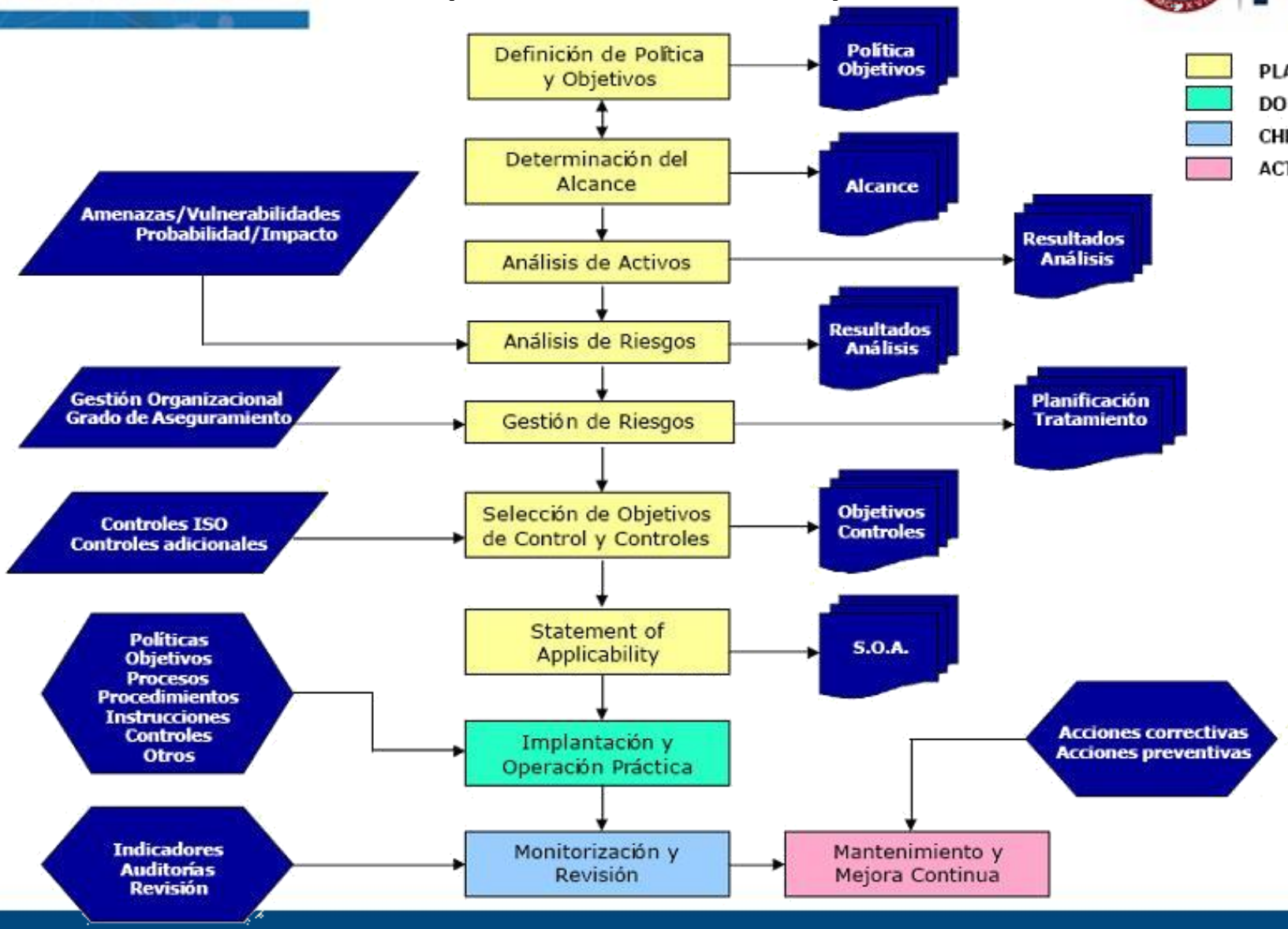
Conceptos

Estableciendo una política de seguridad



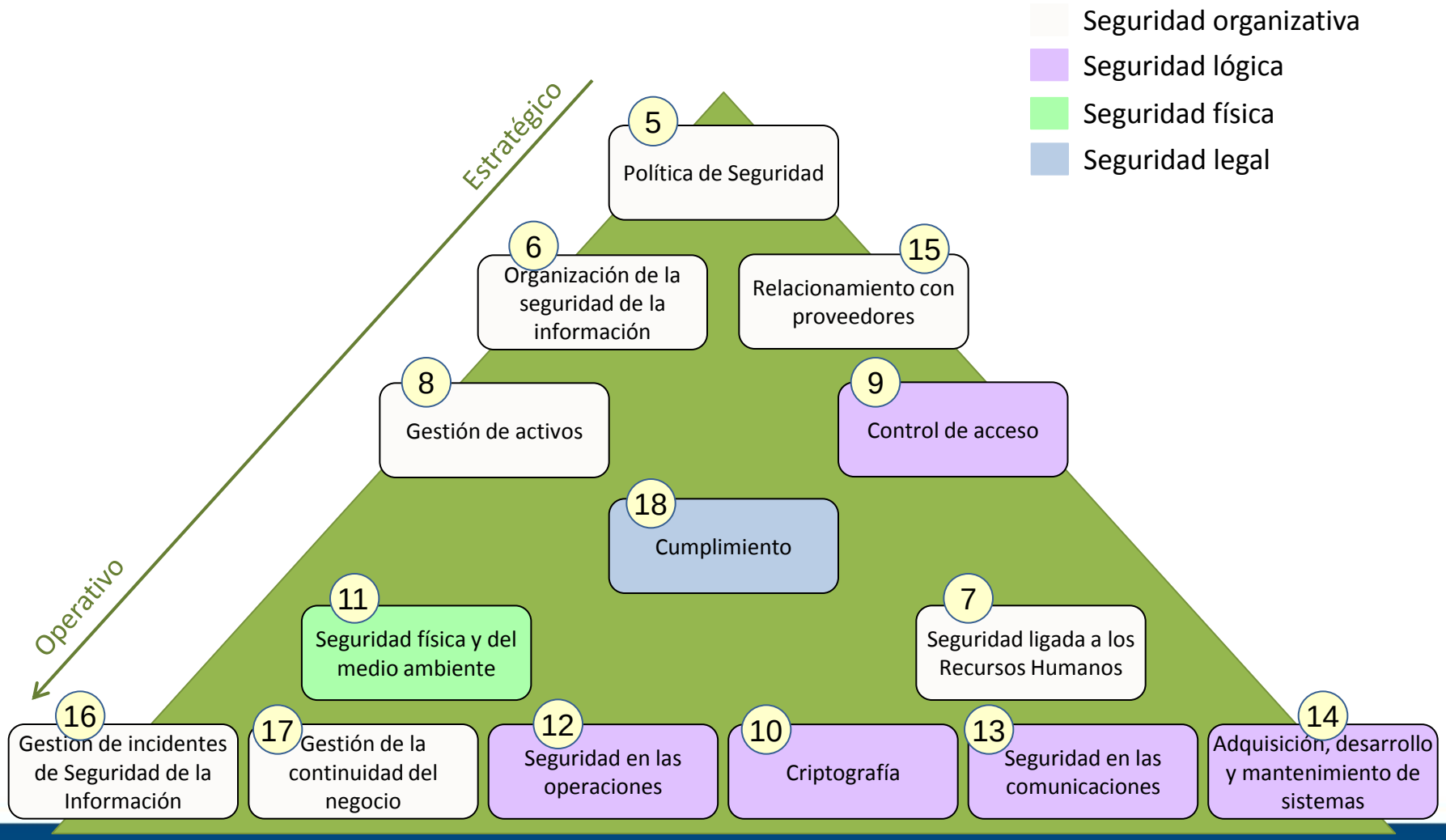
Asignando recursos y concientizando

Siempre, todo será perfectible



NTP 27001:2014

(14 Dominios, 35 Objetivos de control, 114 Controles)



Política de seguridad de la información

A.5

1) Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.

2 Controles

Aspectos organizativos de la seguridad de la información

A.6

1) Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
2) Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.

7 Controles

Seguridad ligada a los recursos humanos

A.7

1) Asegurar que los empleados y contratistas entienden sus responsabilidades y son convenientes para los roles para los que se les considera.
2) Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.
3) Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

6 Controles

A.8

Gestión de activos

1) Identificar los activos de la organización y definir responsabilidades de protección apropiadas.
2) Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización.
3) Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.

10 Controles

Control de accesos

A.9

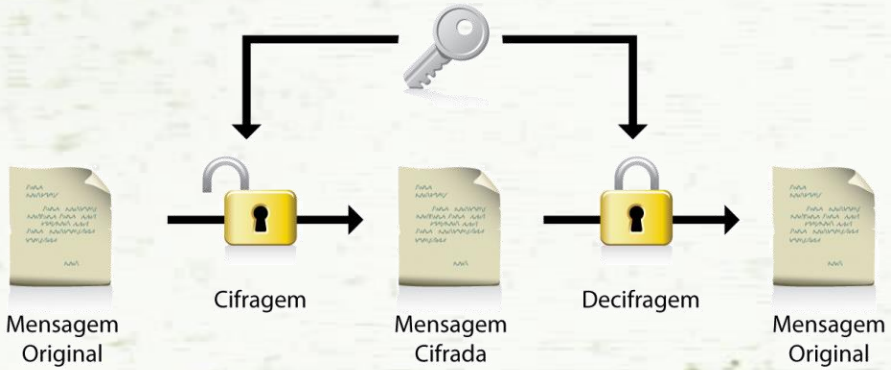
1) Limitar el acceso a la información y a las instalaciones de procesamiento de la información.
2) Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.
3) Hacer que los usuarios respondan por la salvaguarda de su información de autentificación.
4) Prevenir el acceso no autorizado a los sistemas y aplicaciones.

13 Controles

Cifrado

A.10

1) Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.



2 Controles

Seguridad física y ambiental

A.11

1) Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.
2) Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.

15 Controles

Seguridad de las operaciones

A.12

1) Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.
2) Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos
3) Proteger contra la pérdida de datos
4) Registros y monitoreo
5) Asegurar la integridad de los sistemas operacionales
6) Prevenir la explotación de vulnerabilidades técnicas
7) Consideraciones para la auditoría de los sistemas de información

14 Controles

Seguridad en las telecomunicaciones

A.13

1) Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.
2) Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

7 Controles

Adquisición, desarrollo y mantenimiento de los SI

A.14

1) Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.
2) Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
3) Asegurar la protección de datos utilizados para las pruebas.

13 Controles

Relaciones con proveedores

A.15

1) Asegurar protección a los activos de la organización que son accesibles por los proveedores.
2) Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.

5 Controles

Gestión de incidentes en la seguridad de la información

A.16

1) Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.

7 Controles

Gestión de la continuidad del negocio

1) La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización.
2) Asegurar la disponibilidad de las instalaciones y procesamiento de la información.

4 Controles

Cumplimiento

A.18

1) Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.
2) Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.

8 Controles

NTP 27001:2014

(14 Dominios, 35 Objetivos de control, 114 Controles)

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

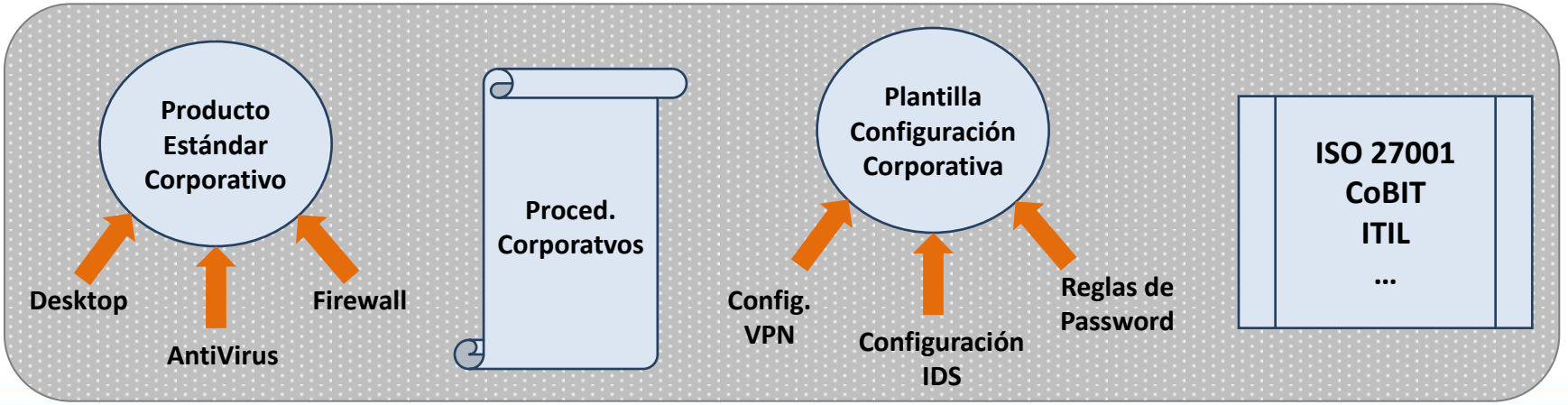
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibiljdad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Implementando la Norma NTP ISO/IEC 27001:2014

A5-Políticas de seguridad de la información

Implementación de las Políticas



¿Cómo logramos nuestro objetivo?

Logremos nuestro Objetivo…

- Creer en los empleados,
- Prevenir las “debilidades naturales” de la política de seguridad,
- Educar a los usuarios en la política y el valor de los activos,
- “Está prohibido hacer eso” (explicar a usuarios porqué),
- Revisar regularmente el cumplimiento de los objetivos,
- Hacer correcciones si es necesario.

Educación de los usuarios

- Campaña de difusión de la seguridad,
- Actualizaciones periódicas,
- Boletines, trípticos, posters…
- Reuniones en Grupos,
- Salvapantallas,
- Firmas digitales,
- Destructor de documentos,
- Auditorías Periódicas,
- “Recompensas”,
- Los “amigos” no son siempre “amigos”.

Concienciación y sensibilización…

Una buena política de seguridad, debe…

- Ser corta (1 o 2 páginas),
- Ser fácilmente comprensible y clara,
- Declarar abiertamente la importancia de la información (y su seguridad) para el negocio,
- Informar a los empleados de sus responsabilidades y cómo usar adecuadamente los recursos de la empresa,
- Sentar la base para su desarrollo en otras políticas funcionales y procedimientos,
- Declarar la existencia de sanciones y recompensas (especificadas en otras políticas de concienciación).

Declaración de Política de Seguridad

Áudea
Seguridad de la Información

MS-02 DECLARACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFROMACIÓN
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
VERSIÓN: 2.1- AÑO: 2011

Política de Seguridad de la Información

La Dirección de Áudea quiere dar a conocer, a través de este documento, a sus trabajadores, clientes, proveedores y otras partes interesadas su convencimiento de que la Seguridad de la Información es un factor clave para el correcto desarrollo de la organización.

Áudea considera que la Gestión de la Seguridad de la Información, junto con la dotación de formación y recursos necesarios para el desarrollo de la actividad propia de la organización, son los principales pilares en los que se fundamenta el trabajo y esfuerzo diario. Todo ello entendiendo por actividad propia de la organización la prestación de servicios Auditoría y Consultoría en Seguridad de la Información.

ADEMÁS, EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN TIENE COMO OBJETIVOS GENERALES:

- Asegurar el cumplimiento de la legislación, reglamentación y normativas aplicables, así como todos aquellos requisitos que la organización considere oportunos llevar a cabo para mantener un Sistema de Gestión de Seguridad de la Información, que le permita conseguir una mejora continua de su actuación.
- Asignación eficaz de funciones y responsabilidades en el ámbito de la seguridad.
- Servicios con un nivel de seguridad de la información que satisfagan y superen las necesidades de nuestros clientes.
- Prevención de posibles defectos y posibles incidentes de seguridad de la información antes de que ocurran, trabajando orientados hacia la "mejora continua" y la comunicación.
- Evolución continua del Sistema de Gestión de Seguridad de la Información, con el fin de adecuarnos a las exigencias de nuestros clientes.
- Concienciación y motivación del personal de Áudea sobre la importancia de la implantación y desarrollo de un Sistema de Gestión de Seguridad de la Información.
- Analizar los riesgos a los que está expuesta la Organización, y gestionarlos de la mejor forma posible para alcanzar el nivel de riesgo aceptado por la Dirección. El SGSI proporciona los mecanismos para, basándose en la metodología MAGERIT 2, analizar y gestionar el riesgo, y determinar aquellos riesgos que la Organización considera aceptables. El nivel de seguridad de Áudea queda establecido por la Dirección en un Acta del Comité de Dirección.

Recordar …

Una sesión formativa NO es suficiente

Actualizaciones periódicas para mantener al personal ATENTO

Evitar ser el enemigo

No te conviertas en otra fuente de "ruido" a ser ignorada

Ser creativos

Transmitir aplicación personal a su vida…

Hacer la Política ACCESIBLE: publícala en una página Web, un tríptico, facilitar su búsqueda

¡Actualízala!

¡Compromiso Dirección!

Taller #4: Alineamiento ISO 27001

- *Instrucciones*:

1) Revise las medidas de mitigación que propuso en el Taller anterior y haciendo uso de la Tabla de controles de la ISO 27001, responda:
    1) Qué objetivos de control de la norma ISO 27001 y de que dominios estarían siendo cumplidos (indique si total o parcialmente) por las medidas de mitigación que propuso
    2) Qué controles de la norma ISO 27001 estarían siendo cumplidas por la medidas de mitigación que propuso

- *Tiempo*: 35 minutos.

FIN

Carlos Trigo Pérez
trigoperezc@gmail.com