#gigatic16

gigaTIC X Congrés Iberoamericà de la Governança i la Gestió Avançada de les TIC

28 abril - Barcelona

Torre Telefónica - Diagonal 00

organitzen:

itSMF ESPAÑA Catalunya

ISACA Trust in, and value from, information systems Barcelona Chapter

Uptc Universidad Pedagógica y Tecnológica de Colombia

proactivanet ITSM SOFTWARE

CASO DE EXITO EN LA CERTIFICACION ISO 20000-1:2011 E ISO 27001:2013 EN LA UPTC UNA UNIVERSIDAD PUBLICA COLOMBIANA

Diana Rocío Plata Arango

Sessió P7

#gigaTIC16

"La innovación no tiene nada que ver con cuantos dólares has invertido en I+D. Cuando Apple apareció con el Mac, IBM gastaba al menos 100 veces más en I+D. No es un tema de cantidades, sino de la gente que posees, cómo les guías y cuánto obtienes". - ***Steve Jobs***

INTRODUCCION

Introducción.

- El Reto de asumir la certificación en ISO 20000-1:2011 e ISO 27001:2013.
- Ser la primera Universidad en Latinoamérica.
- El modelo propuesto
- Los Indicadores.

ISO 20000-1:2011

ISO 20000:1-2011

- Es un estándar para la Gestión de servicios, La norma ISO 20000 se centra en la integración y aplicación de los procesos coordinados de gestión de servicios. Su objetivo es proporcionar un control continuo, una mayor eficiencia y oportunidades para seguir mejorando.
- **Eso significa trabajar dentro de la organización para alinear el personal y los procedimientos de su servicio al cliente, servicios de apoyo, prestación de servicios y equipo de operaciones.**

- fuente http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/Risk-Assessment-and-Management/Security-Management/ISO-20000-IT-Certification.aspx

ISO 20000:1-2011

- La certificación ISO 20000 demuestra la fiabilidad y calidad de sus servicios de TI a los empleados, accionistas y clientes., Además que cumple con los "Requerimientos necesarios para realizar una entrega de servicios de TI alineados con las necesidades y objetivos del negocio, con calidad y valor añadido para los clientes"
- https://www.aenor.es/AENOR/certificacion/calidad/calidad_serviciosti_20000.asp#.VSsp0_mG85k

ISO 20000:1-2011

- Un beneficio adicional, además de la satisfacción de los usuarios es lograr el cambio de percepción en que las áreas de Tecnología son sólo costos, pues con la adopción de buenas prácticas bajo los estándares internacionales se puede evidenciar, como los departamentos de tecnología le agregan valor a la organización y permiten que sean más eficientes en el uso planificado y controlado de los recursos requeridos, ventajas que se pueden obtener con ISO 20000.

SYSTEM CERTIFICATION
ISO 27001
SGS
CO15/6074

ISO 27001:2013

itSMF ESPAÑA Catalunya

gigaTIC 16

ISACA Trust in, and value from, information systems Barcelona Chapter

ISO 27001:2013

- ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.
- http://www.iso27001standard.com/es/que-es-iso-27001/

ISO 27001:2013

- El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

ISO 27001:2013

- Asegurar la confidencialidad, disponibilidad e Integridad de la Información, y esto representa enormes beneficios tanto para la organización como para los usuarios finales, ya que se puede lograr disminuir incidentes de seguridad de la información que en la actualidad son tan comunes, como los fraudes a través de correo electrónico y redes sociales, y se debe brindar información a los usuarios para que conozcan y asuman el reto que **la responsabilidad de la seguridad de la Información es tarea de todos**.

MODELO DE IMPLEMENTACION PROPUESTO

ALCANCE

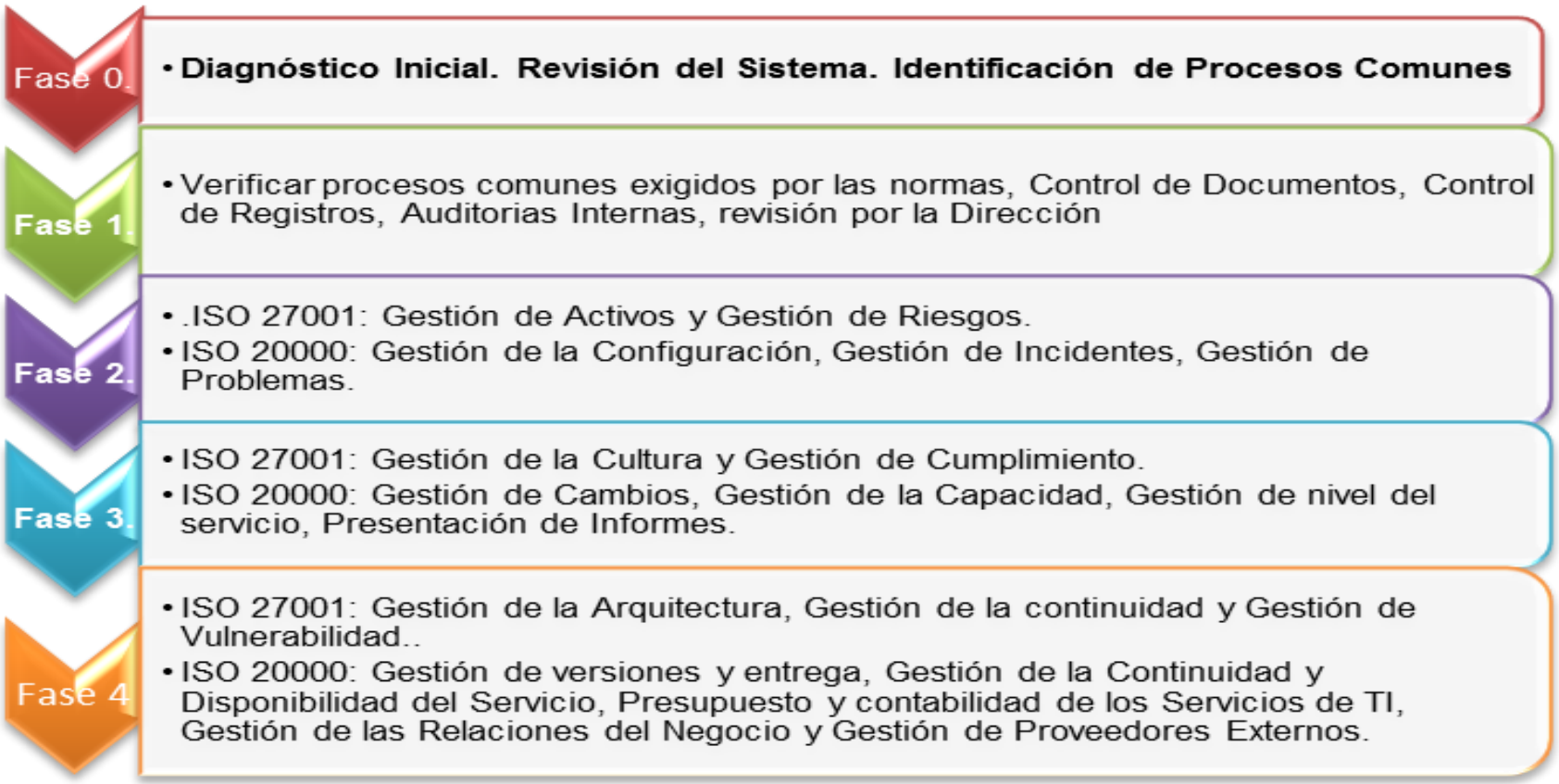
- En la Universidad se eligió El proceso Gestión de Recursos Informáticos para el alcance de las normas que hace parte de los procesos administrativos dentro del Sistema de calidad. Este proceso es el que contempla las actividades realizadas actualmente en el Grupo Organización y Sistemas que tiene definidas 4 áreas de trabajo:
- Desarrollo y administración de los sistemas de Información,
- Redes y Telecomunicaciones
- Soporte a Usuarios en Hardware y Software.
- Administración de aulas de Informática para préstamo a Docentes y estudiantes.

ALCANCE

- El objetivo del proceso es: *"Gestionar La Infraestructura Informática Y De Telecomunicaciones, Que Permita La Prestación De Servicios cumpliendo con las políticas de Seguridad de la Información Para La Satisfacción De Necesidades De Los Clientes"* [3] y en este objetivo se refleja la incorporación de Seguridad y de servicios requeridos por ISO 20000 e ISO 27001.

- El proceso contaba inicialmente con cuatro (4) procedimientos que integraban el quehacer básico del Grupo Organización y Sistemas dentro de la Universidad Pedagógica y tecnológica de Colombia, y con la implementación de las normas han pasado a ser ahora veintisiete (27).

MODELO PROPUESTO



Fases para la implementación de servicios con las normas ISO 2000 e ISO 27000, luego del Análisis GAP. Fuente Autor.

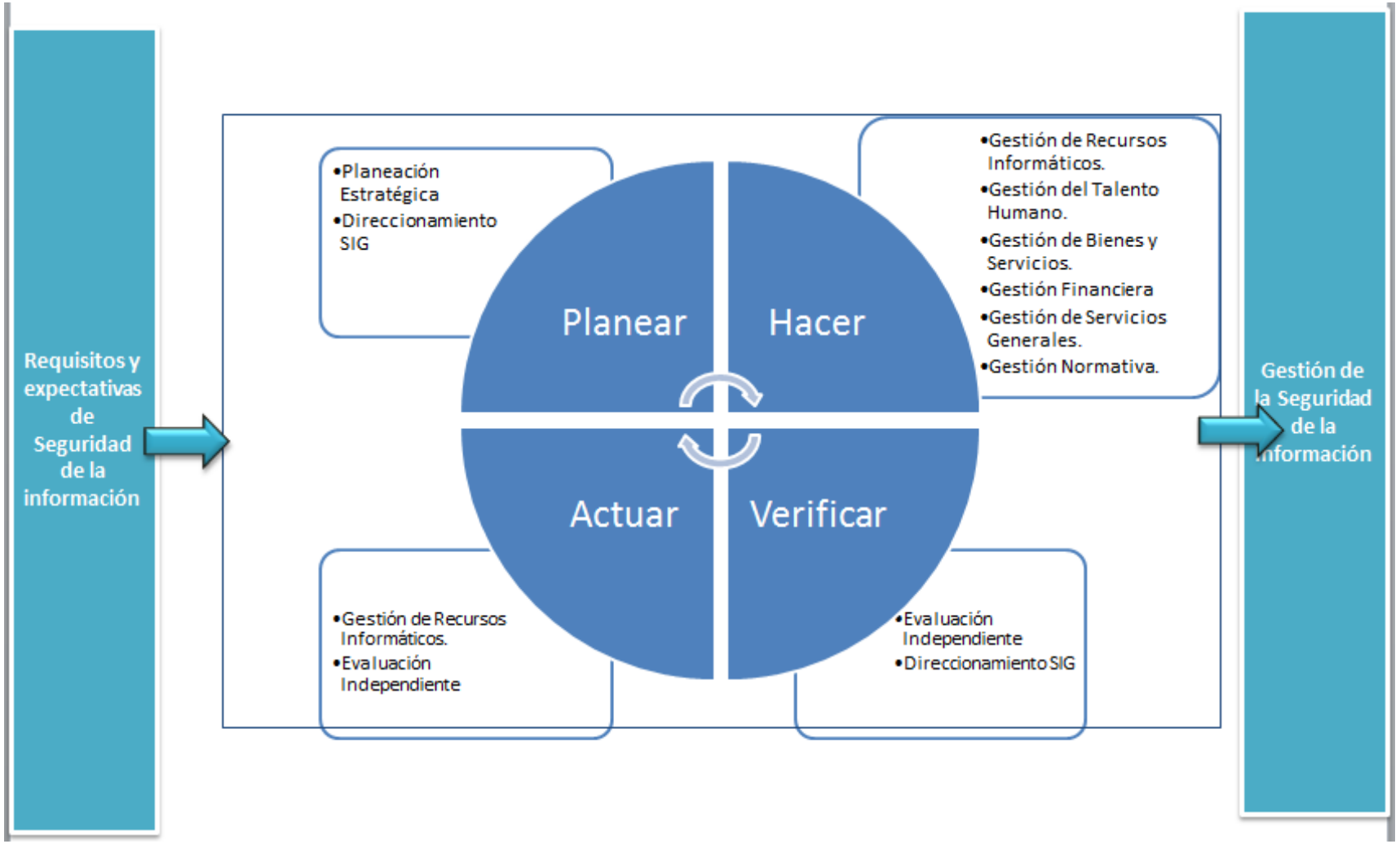
MODELO PROPUESTO

- Este modelo, permitió llevar un hilo conductor de como ir avanzando en la implementación de los procedimientos, sin embargo a la par era necesario ir reforzando las estrategias para lograr realizar no solo la implementación sino también la certificación,
- La primera estrategia fue contar con el apoyo de la alta dirección, luego de esto es importante asegurar recursos para capacitar al personal de TI en los fundamentos de las normas y en auditoría a las mismas, así mismo se deben disponer recursos para la contratación de las empresas consultoras o expertos que colaboren en el proceso.

Mapa de Procesos SGS.

- Se estableció el catálogo de servicios del área y con ellos se definió el alcance para la certificación:
- Desarrollo de aplicaciones.
- Asistencia Técnica.
- Aulas de Informática.
- Infraestructura de Red y comunicaciones.
- Gestión de la seguridad informática.
- Y para cada uno de ellos se generó el respectivo acuerdo de nivel de servicio.

MAPA DE PROCESOS SGSI



HITOS EN EL PROCESO DE IMPLEMENTACIÓN PARA EL ÁREA DE TI.

10 Hitos Para El Área De TI.

- **1. Capacitar al personal de TI**. Se buscó capacitación certificada en Fundamentos de la norma ISO 20000 y la norma ISO 27001 para todos. No todos pasaron los cursos, fue necesario repetir durante los tres años los fundamentos de las normas para generar conciencia y motivación, y aún hoy es necesario, para dejar ver que no es una moda sino un cambio en la manera de hacer.

10 Hitos Para El Área De TI.

- **2. Identificar capacidad y disponibilidad de TI**, para prestar los servicios. Implica no hablar solamente de un inventario de elementos de TI, sino identificar como están asociados a recursos humanos y financieros y que disponibilidad presentan para atender los servicios.
- selección de Herramientas de Software – Proactiva Net.

10 Hitos Para El Área De TI.

- **3. Pasar de atender solicitudes de soporte a atender incidencias o peticiones a través de la Mesa de Ayuda**. Tener en cuenta los acuerdos de niveles de servicio, registrar y clasificar de acuerdo al servicio. Atender las incidencias considerando los tiempos establecidos.
- Selección de Herramientas de Software – Proactiva Net.

10 Hitos Para El Área De TI.

- **4. Identificar incidentes de seguridad y registrarlos**. Aprender a identificar y clasificar los incidentes de seguridad y llevar el debido registro.

- Selección de Herramientas de Software – Proactiva Net.

10 Hitos Para El Área De TI.

- **5. Solicitar Auditorías Externas para gestión de Vulnerabilidades**. Considerar que se pueden tener vulnerabilidades y abrir el espacio para que un tercero entre a verificar las condiciones de acceso a equipos y sistemas de información, cuando antes se consideraba que todo estaba bien

10 Hitos Para El Área De TI.

- **6. Preparar la Gestión de Continuidad**. Pensar en cómo iniciar a tener un plan de recuperación de desastres como una primera estrategia de garantizar continuidad, cuando no se tenía ninguna opción y revisando presupuesto

10 Hitos Para El Área De TI.

- **7. Identificación de activos de información y Valoración de Riesgos de Seguridad de la Información**. Comenzar a identificar activos de información no solo como equipos, sino considerar las personas y los documentos con un valor especial y los riesgos a los que puede estar expuesto por la información que puede manejar.

10 Hitos Para El Área De TI.

- 8. **Medir, definir indicadores para cada norma**. La medición es un factor importante para evidenciar el cumplimiento del ciclo PHVA, pero identificar que medir y cómo medir es una tarea compleja al iniciar.

10 Hitos Para El Área De TI.

- **9. Auditorías Internas y Externas.** Es necesario que se contraten con consultores externos o empresas expertas, dado que no hay personal suficiente con conocimiento en las dos normas al interior de la organización.

10 Hitos Para El Área De TI.

- **10. Cultura de Seguridad de la Información**. Dar a conocer que la Seguridad es responsabilidad de todos es una tarea que involucra mantener diferentes estrategias involucrar de manera especial a la oficina de comunicaciones.

INDICADORES

INDICADORES SGS.

NUMERO	NOMBRE DEL INDICADOR	FRECUENCIA	FORMULA	META	DATO 1	DATO 2	INDICADOR AL 31/12/2014	DATO 1	DATO 2	INDICADOR 1ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 2DO. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 3ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 4TO. TRIMESTRE 2015
1	Cumplimiento de los acuerdos de nivel de servicio	TRIMESTRAL	100 - (SLA caducados/ SLA reportados*100)	80				SLA Reportados	SLA Caducados	81,6	SLA Reportados	SLA Caducados	80,3	SLA Reportados	SLA Caducados	67,6	SLA Reportados	SLA Caducados	80,4
								1145	211		1185	233		849	275		934	183	
2	Oportunidad atención de incidencias	TRIMESTRAL	Sumatoria Tiempo de resolucion por Tipo / No de items.	6					SumaTpoResportipo/ No. Items	9,8		SumaTpoResportipo/ No. Items	5,5		SumaTpoResportipo/ No. Items	6,0		SumaTpoResportipo / No. Items	9,8
									9,81			5,4925			5,97			9,822	
3	Disponibilidad de los servicios El tiempo de disponibilidad mensual son 160 horas	MENSUAL	100 - (Tiempo indisponibilidad mensual *100/ tiempo total de servicio)	90				480	36	92,5	480	32	93,3	480	64	86,7	480	20	95,8
					Porcentaje de cumplimiento mensual.			92,5	95	90	95	90	95	91,25	75	93,75	95	98,75	
		reporte de horas indisponibles de cada mes		160	No. de horas indisponibles mensual			12	8	16	8	16	8	14	40	10	8	2	
4	Satisfacción de usuarios	TRIMESTRAL	(Número de usuarios satisfechos con el servicio / Número total de usuarios encuestados)* 100%	90	NUS	NTUE		NUS	NTUE	92,0	NUS	NTUE	99,1	NUS	NTUE	97,5	NUS	NTUE	96,1
					1389	1442	96,3	759	825		541	546		868	890		1397	1454	

INDICADORES SGS

NUMERO	NOMBRE DEL INDICADOR	FRECUENCIA	FORMULA	META	DATO 1	DATO 2	INDICADOR AL 31/12/2014	DATO 1	DATO 2	INDICADOR 1ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 2DO. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 3ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 4TO. TRIMESTRE 2015
5	Planes de mantenimiento de equipos y actualización de tecnología	SEMESTRAL	(Mantenimientos ejecutados / Mantenimientos planeados)*100%	90	ME 691	MP 691	100,0	ME 0	MP 0	0,0	ME 340	MP 340	100,0	ME 0	MP 0	0,0	ME 245	MP 253	96,8
6	Actualización de tecnología	ANUAL	(Equipos actualizados / Equipos planeados para actualizar)*100 %	90	EA 7	EP 7	100,0	EA 0	EP 0	0,0	EA 0	EP 0	0,0	EA 0	EP 0	0,0	EA 25	EP 25	100,0
7	cumplimiento Plan de Acción. * en 2015 comienza a partir de trimestre por formulación plan de desarrollo.	TRIMESTRAL	Sumatoria del porcentaje de cada actividad/ número total de actividades del trimestre.	85												85,7			96,7
8	Usuarios Beneficiados con la soluciones de TI. primer Trimestre. Solución Voto electrónico. Segundo Trimestre. Inclusión de aulas de informatica (8) Tercer Trimestre. Autenticación con LDAP en red inalámbrica. Diseño nuevo de la red. Cuarto Trimestre. Simulador para Admisiones uso de aspirantes. Sistema Integrado de PQR.	TRIMESTRAL	No. de soluciones de TI Implementadas No. Usuarios Beneficiados con la solución de TI implementadas ./ No. Total de usuarios de la población beneficiada * 100	80	NUB 28000	NTU 31000	90,3	NUB 7282	NTU 9000	1,0 80,9	NUB 28000	NTU 31000	1,0	NUB 29000	NTU 33000	1,0 90,3	NUB	NTU	2.0 87,9

INDICADORES SGS

NUMERO	NOMBRE DEL INDICADOR	FRECUENCIA	FORMULA	META	DATO 1	DATO 2	INDICADOR AL 31/12/2014	DATO 1	DATO 2	INDICADOR 1ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 2DO. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 3ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 4TO. TRIMESTRE 2015
9	**N**úmero de incidentes atendidos	TRIMESTRAL	(Número de incidencias Atendidas / Número de incidencias Reportadas)*100%	80	NIA 1043	NIR 1221	85,4	NIA 93	NIR 130	71,5	NIA 169	NIR 211	80,1	NIA 118	NIR 146	80,8	NIA 90	NIR 101	89,1
	volumen de incidentes volumen de peticiones		volumen de incidencias volumen de peticiones							5,7 16,3			3,3 15,3			3,3 11,1			1,7 12,8
10	**N**úmero de peticiones atendidas	TRIMESTRAL	(Número de peticiones atendidas / Número de peticiones reportadas)*100%	70	NPA 1357	NPR 1504	90,2	NPA 828	NPR 1037	79,8	NPA 782	NPR 986	79,3	NPA 494	NPR 726	68,0	NPA 892	NPR 910	98,0
11	**N**úmero de Mejoras Implementadas	TRIMESTRAL	(Número de mejoras implementadas / Número de mejoras programadas) *100%	80	NMI 3	NMP 3	100,0	NMI 4	NMP 4	100,0	NMI 2,5	NMP 3	83,3	NMI 2,5	NMP 3	83,3			83,3

itSMF ESPAÑA Catalunya

INDICADORES SGSI

N°	NOMBRE DEL INDICADOR	FRECUENCIA	FORMULA	META	DATO 1	DATO 2	INDICADOR AL 31/12/2014	DATO 1	DATO 2	INDICADOR 1ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 2DO. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 3ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 4to. TRIMESTRE 2015
1	Verificación del Mejoramiento del SGSI	TRIMESTRAL	(NNC/NTNC)*100%	80	NNC	NTCN *	97,2	NNC	NTCN *	42,9	NNC	NTCN *	85,7	NNC	NTCN *	85,7	NNC	NTCN *	80,0
					35	36		3	7		6	7		6	7		12	15	
2	Revisión de Políticas	ANUAL	No. de revisiones realizadas	>=1									1,0						1,0
3	Efectividad del plan de Tratamiento de Riesgos	SEMESTRAL	(SUMATORIA%NPI/NPP)	85	NPI	NPP	88,8	NPI	NPP	N.A.	NPI	NPP	87,5	NPI	NPP	N.A.	NPI	NPP	93,3
					1420	16		0	0		14	16					14	15	

INDICADORES SGSI

N°	NOMBRE DEL INDICADOR	FRECUENCIA	FORMULA	META	DATO 1	DATO 2	INDICADOR AL 31/12/2014	DATO 1	DATO 2	INDICADOR 1ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 2DO. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 3ER. TRIMESTRE 2015	DATO 1	DATO 2	INDICADOR 4to. TRIMESTRE 2015
4	Tratamiento de Incidentes de Seguridad de la Información	TRIMESTRAL	(NIS/NIR)*100%	90	NIS	NIR	40,9	NIS	NIR	100,0	NIS	NIR	100,0	NIS	NIR	95,0	NIS	NIR	100,0
					277	678		2	2		23	23		19	20		15	15	
5	Medidas preventivas implementadas como respuestas a amenazas.	SEMESTRAL	Sumatoria medidas preventivas sobre los activos de información.	>=3	TEI	TEP	N.A.	TEI	TEP	N.A.	TEI	TEP	100,0	TEI	TEP	N.A.	TEI	TEP	100,0
					0	0		0	0		3	3		0	0		2	2	
6	Estrategias de Divulgación del Sistema de Gestión de Seguridad de la Información	SEMESTRAL	(TEI/TEP)*100%	85	TEI	TEP	100,0	TEI	TEP	N.A.	TEI	TEP	100,0	TEI	TEP	N.A.	TEI	TEP	100,0
					4	4					3	3					3	3	

Patrón para encabezado de sección

Conclusiones?

Patrón para encabezado de sección

Preguntas?

Sessió P7

CASO DE EXITO EN LA CERTIFICACION ISO 20000-1:2011 E ISO 27001:2013 EN LA UPTC UNA UNIVERSIDAD PUBLICA COLOMBIANA

Detalls Contacte

Uptc
Universidad Pedagógica y Tecnológica de Colombia

Nom del ponent
Diana Rocio Plata Arango.

Adreça Correu
Diana.plata@uptc.edu.co

Telèfon Contacte
573108840204

Twitter
@diana7428