



Recomendaciones para Mitigar Riesgos

11 de noviembre de 2011

Azucena Navas C.

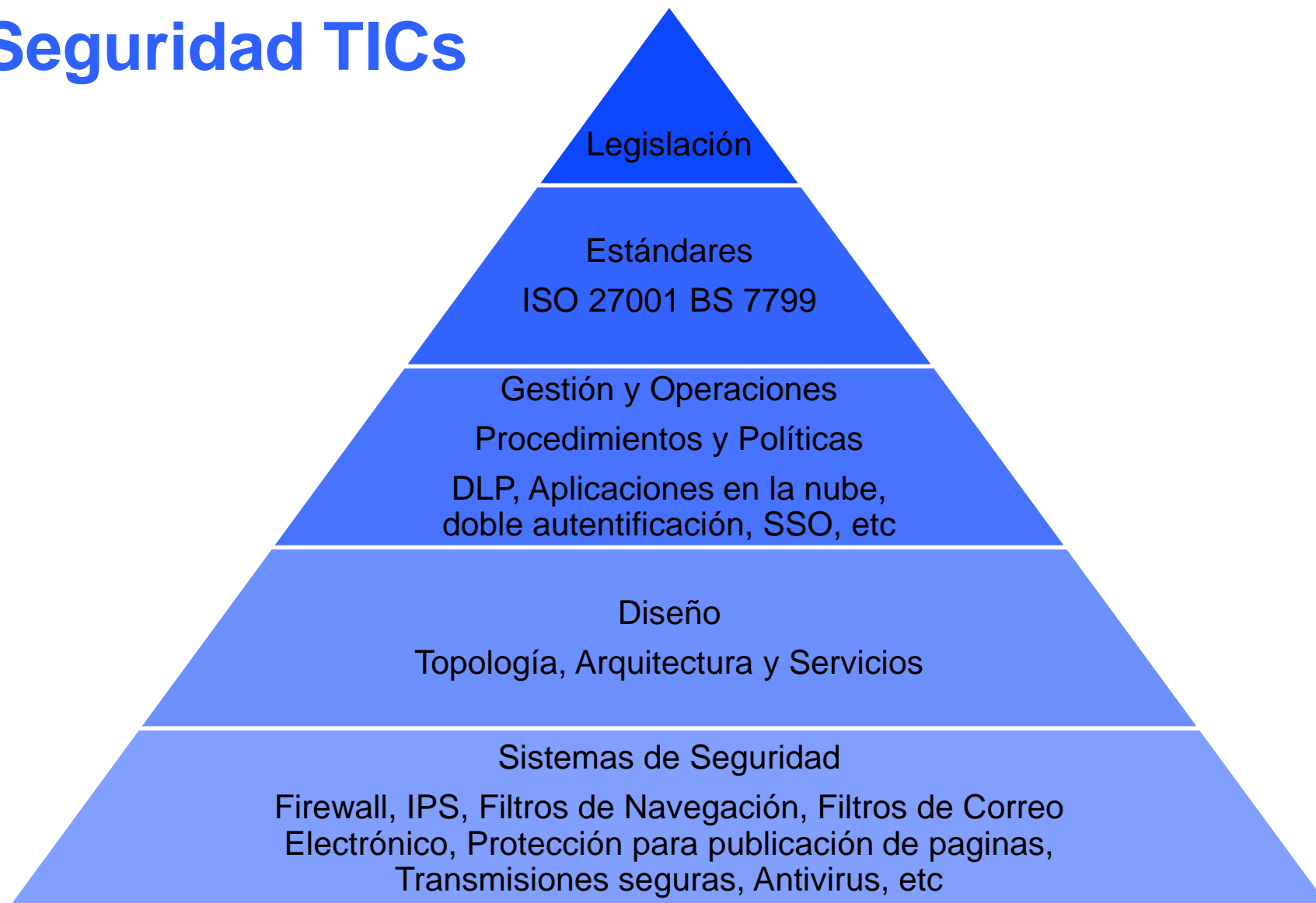
Agenda

- Seguridad Informática
- Estructura Base de Seguridad TICs
- Errores comunes: Primera etapa de mitigar riesgos

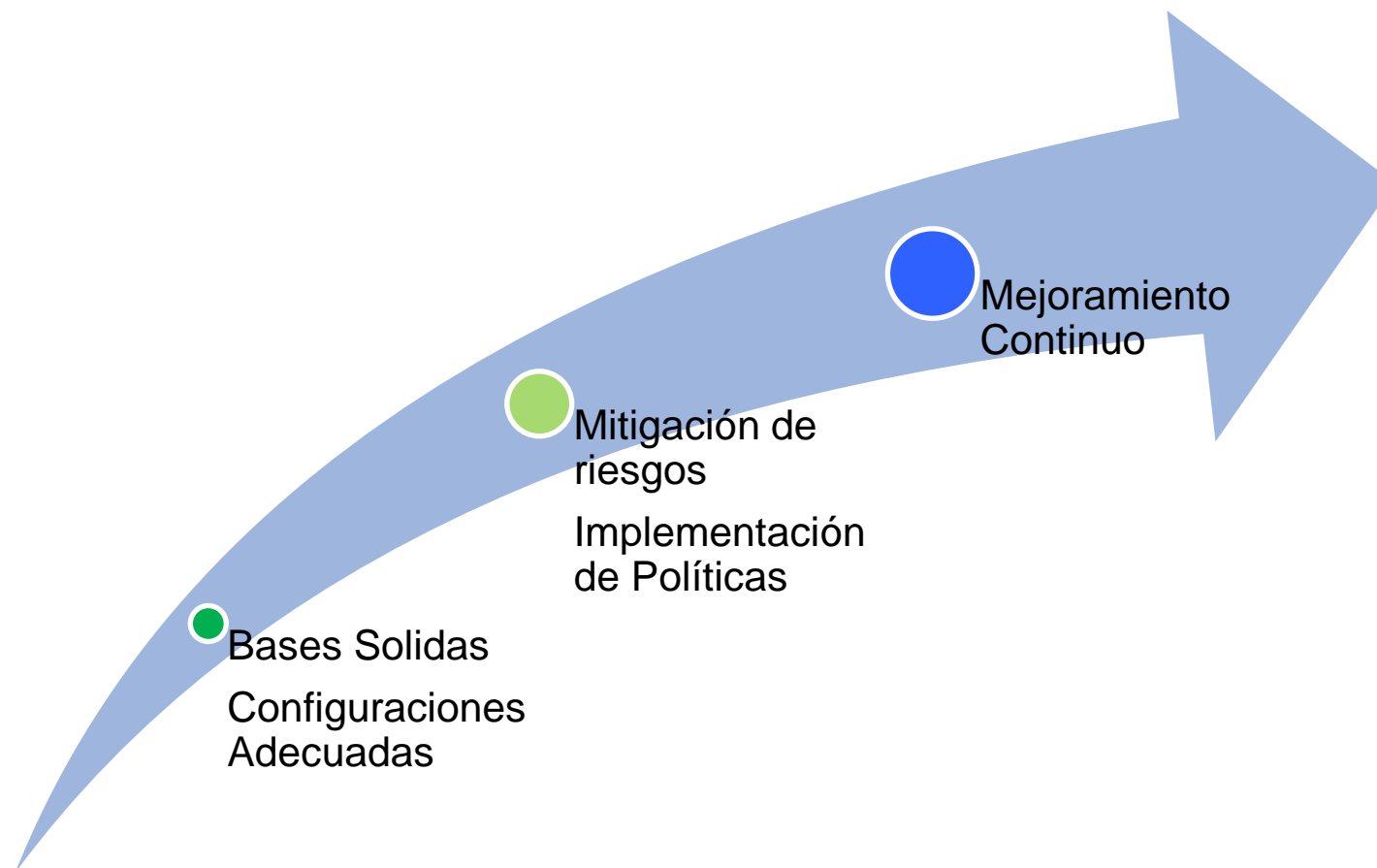
Seguridad Informática



Seguridad TICs

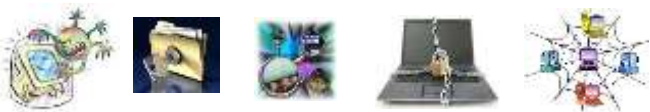
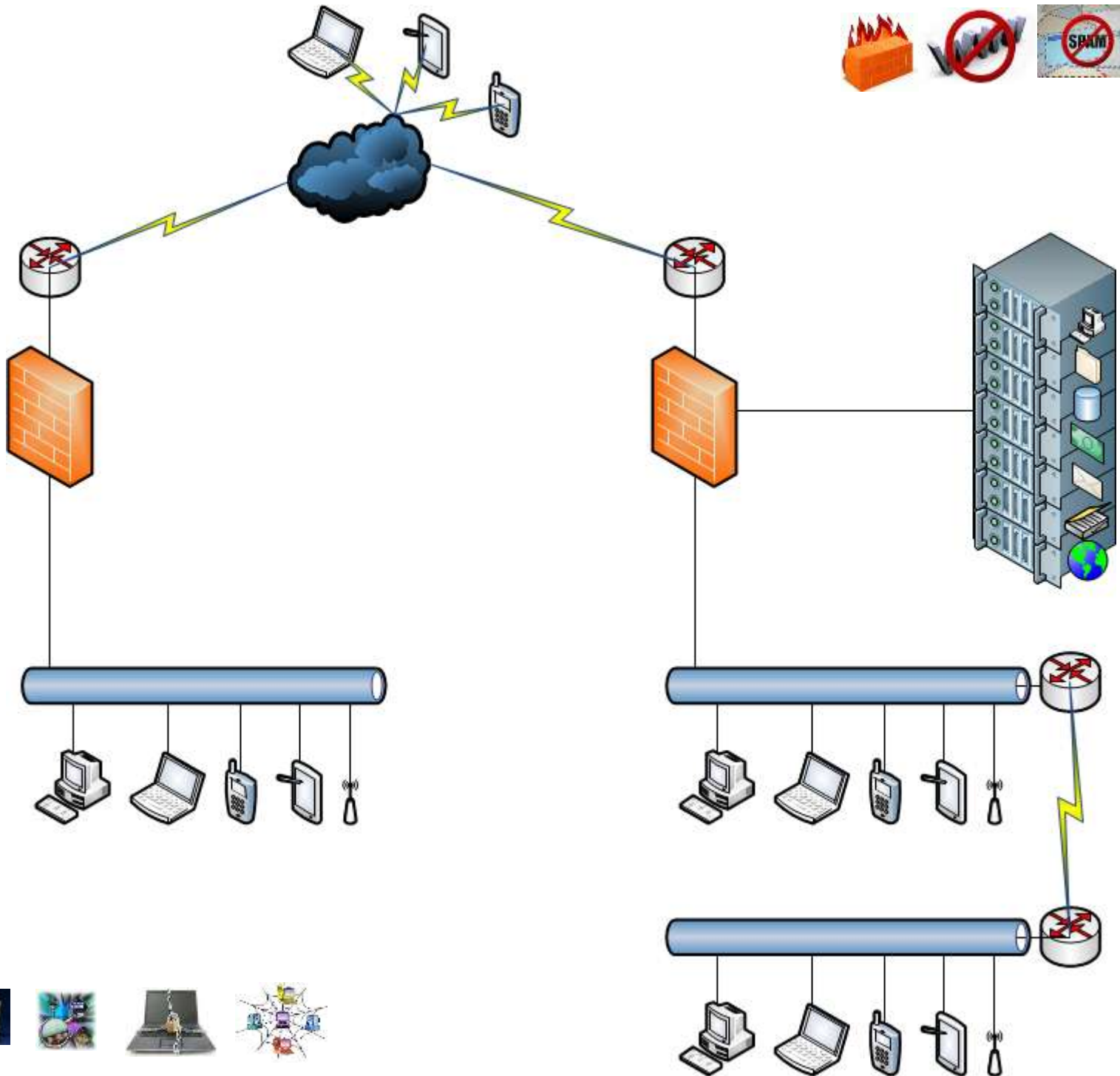


Seguridad TICs



Estructura Base de Seguridad TICs





Errores comunes

Primera etapa de mitigar riesgos



Errores Comunes: Sistemas de seguridad Desactualizados

Tener en cuenta

- Active las opciones de actualización automática
- Instale los parches publicados por el fabricante para evitar vulnerabilidades conocidas
- Mantenga visibilidad de las actualizaciones que están pendientes
- Asegúrese de tener un backup fácil de recuperar en caso de que la actualización falle

Errores Comunes: Debilidades en la Administración de soluciones de seguridad

Tener en cuenta:

- Mantenimiento de usuario
 - Altas, permisos de acceso y bajas correctas
- Mantenimiento de configuración
 - Revisión periódica / auditoria interna de las reglas de configuración
- Monitoreo
 - En lo posible monitoreo en tiempo real para prever posibles problemas en el equipamiento y su comportamiento.

Errores Comunes: Conectar sistemas TI a Intranet o Internet antes de protegerlos

Tener en cuenta

Usuarios Finales:

- Antivirus institucional debidamente instalado, actualizado e integrado a la consola de administración
- Usuarios validos debidamente dados de alta en los sistemas, teniendo especial cuidado en el nivel de acceso a la información que manejan

Errores Comunes: Conectar sistemas TI a Internet antes de protegerlos

Tener en cuenta

Servidores (ej.: Portal institucional, Webmail)

- Protección de URLs y formularios
- Protección de vínculos
- Prevención de escalado de directorios
- Protección contra inyección de SQL
- Protección contra Cross-Site Scripting
- Motores antivirus
- Cookies con firmas digitales

Errores Comunes: Conexiones externas hacia la red sin protección

Tener en cuenta

- Uso de alternativas seguras de conexión como VPN
- Manejar Control de Acceso remoto que permita aplicar las políticas de la institución
- Utilizar algoritmos de encriptación que permitan manejar conexiones seguras
- Mantener logs de actividades de usuarios externos

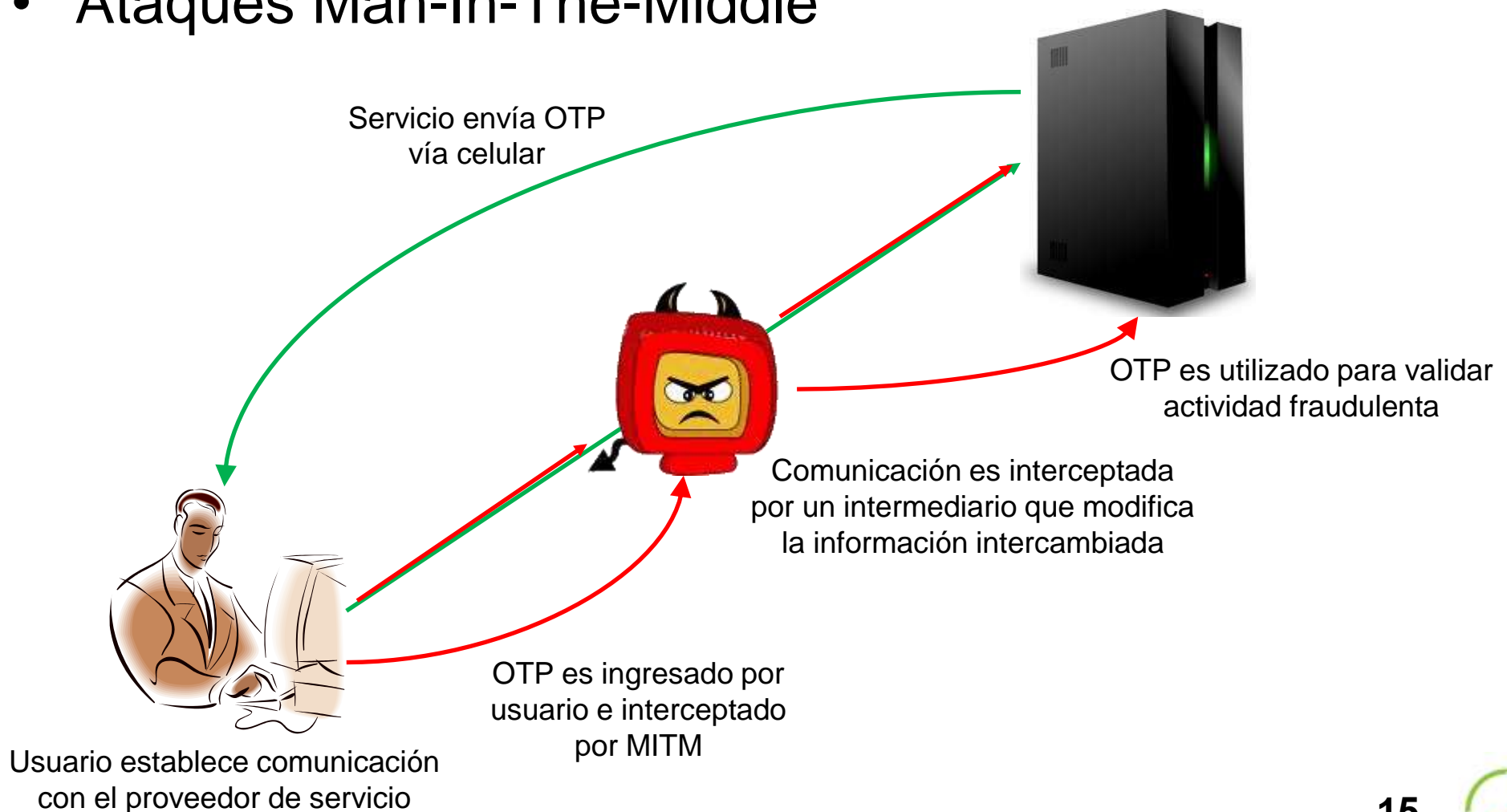
Errores Comunes: Conexiones externas hacia la red sin protección

Tener en cuenta

- Asegurar que la conexión permite la integridad, confidencialidad y seguridad de los datos.
- Mantenga factores de doble autenticación, tales como: Preguntas personales / Contraseñas / pines de uso único / dispositivos alternos (OTP)
- Independencia de medios o líneas de comunicación para factores de doble autenticación

Out-of-band: un elemento clave

- Ataques Man-In-The-Middle



Out-of-band: un elemento clave

- Independencia real de canales

Servicio envía OTP a un celular
vía servicio de datos



Usuario valida su autenticación
por el mismo canal independiente



Usuario establece comunicación
con el proveedor de servicio



MITM podrá vulnerar un canal de
comunicación, pero no los dos



Errores Comunes: Oficinas remotas que no cumplen políticas de seguridad institucional

Tener en cuenta

- Gestión centralizada
- Túnel cifrado o Uso de certificados digitales
- Filtrado centralizado integrado a la solución de matriz
- Gestión de recursos de manera extendida como si fuera la misma red

Errores Comunes: Redes Sociales sin controles

Tener en cuenta

- Control de aplicaciones y patrones de Nivel 7
- Monitoreo de tráfico en tiempo real
- Permita Analizar malware
- Cuento con Filtro de contenido activo
- Cuento con Detección de spyware
- Permita Políticas de acceso basadas en horas, usuarios y grupos
- Cuento con Filtro por autenticación en tiempo real

Errores Comunes: Redes inalámbricas sin protección

Tener en cuenta

- Gestión centralizada
- Seguridad integrada a la solución principal de seguridad
- Busque que proteja de forma instantánea puntos de acceso y clientes inalámbricos
- Debe permitir cifrado en la comunicación
- Asegure acceso seguro a Internet para invitados, sin afectar la seguridad de la red institucional

Errores Comunes: Cambios de los administradores de Seguridad sin auditoria

Tener en cuenta

- Realizar seguimiento de cambios de configuración
- Almacenar los registros con detalle de pistas de auditoría que al menos indiquen fecha y hora, usuario, configuración anterior, configuración actual.
- Administración de perfiles que permitan generar varios niveles de administradores.

Errores Comunes: Actividad de usuarios no monitoreada o reportada

Tener en cuenta

- Generación de informes detallados
- Permita enviar por correo electrónico los informes
- Permita exportación de informes como PDF
- Permita archivado de logs en sistemas externos
- Generación de informes consolidados de la actividad diaria
- Seguimiento y auditoría por usuario

Errores Comunes: Ausencia de conciencia de seguridad en los usuarios

Tener en cuenta

- Comunique las políticas de seguridad de la empresa
- Capacite acerca del buen uso de la información, incluyendo usuarios y claves
- Transfiera la responsabilidad de la propiedad de la información a sus verdaderos dueños
- Aplique las sanciones de las políticas.

¡Muchas gracias por su asistencia!



Consultoría TI
Telecomunicaciones
Seguridades

www.gms.com.ec
info@gms.com.ec
Quito: 292-3500
Guayaquil: 263-0400

