Centro de Especializaciones Noeder

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR ISO 27001 E ISO 22301

CICLO INTENSIVO

MÓDULO II

IMPLEMENTACIÓN DE LA NORMA ISO 27001-2022

Ing. Johnattan Sifuentes Rojas

MODULO II – IMPLEMENTACIÓN DE LA NORMA ISO 27001 - 2022

CONTENIDO MODULO I

1. Gestión del contexto organizacional
2. Liderazgo y compromiso en el SGSI
3. Planificación del SGSI
4. Gestión de objetivos y planificación de cambios
5. Gestión de recursos
6. Gestión de la comunicación y documentación
7. Gestión de operaciones
8. Gestión del riesgo operacional
9. Evaluación de desempeño
10. Mejora continua

ALCANDE DEL SGSI

ISO 27001
Sistema de Gestión de la Seguridad de la Información SGSI

GESTION DEL CONTEXTO DE LA ORGANIZACION

1 Establecer el contexto de la organización

Análisis Interno y externo

Partes Interesadas

Necesidades y expectativas

PLANIFICACION SGI

2 Definir el alcance SGSI

Para establecer el **alcance de un SGSI** se puede seguir un enfoque multietapas:

DETERMINAR EL ALCANCE PRELIMINAR	Esta actividad la debería llevar a cabo un grupo pequeño pero representativo de representes de la dirección.
DETERMINAR EL ALCANCE PERFECCIONADO	Las unidades funcionales dentro y fuera del alcance preliminar se deberían revisar, y posiblemente luego se deberían incluir o excluir algunas de estas unidades funcionales para reducir el número de interfaces a lo largo de los límites.
DETERMINAR EL ALCANCE FINAL	El alcance perfeccionado debería ser evaluado por toda la dirección dentro del alcance perfeccionado. Si es necesario, se debería ajustar y luego describir con precisión.
LA APROBACIÓN DEL ALCANCE	La información documentada que describe el alcance la debería aprobar formalmente la alta dirección.

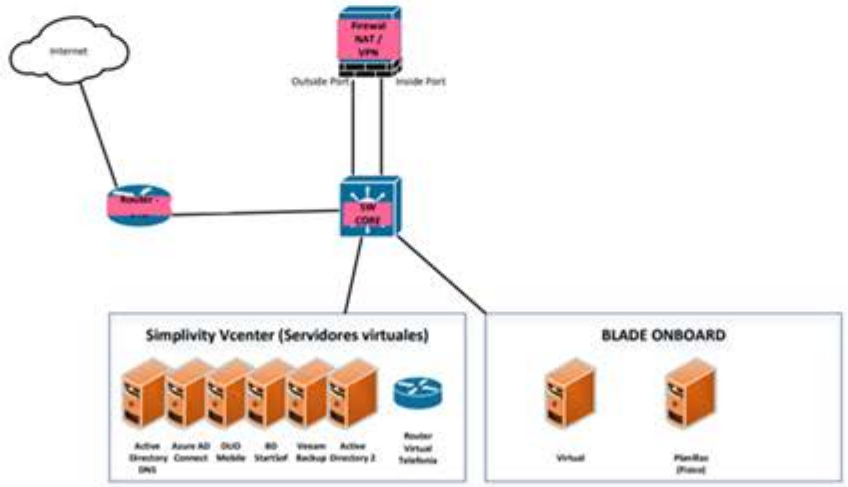
PLANIFICACION SGI

2 Definir el alcance SGSI

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los sistemas de información que dan soporte a los procesos del negocio:

Comercialización y configuración de software contable xxx.
De acuerdo con el documento de aplicabilidad vigente a la fecha de emisión del certificado.



GESTION DE OBJETIVOS Y PLANIFICACIÓN DE CAMBIOS

3 Establecer Politica y Objetivos SGSI

Nube SAC es una empresa especializada en la comercialización de software as a service, nos comprometemos a mantener un Sistema de gestión de seguridad bajo los siguientes pilares:

Compromiso de la dirección: La dirección de la empresa se compromete a proporcionar los recursos necesarios para implementar y mantener esta política.

Responsabilidad: Cada empleado es responsable de proteger la información de la empresa.

Cumplimiento de requisitos aplicables: La empresa cumplirá con todas las leyes, regulaciones y requisitos del cliente en materia de seguridad de la información.

Mejora continua: El SGSI se evaluará y mejorará continuamente.

Objetivos de la ISO 27001

GESTION DE RECURSOS

5 Proporcionar recursos
Personal competente

CISCO

Resumen de responsabilidades, acciones y métricas

Responsabilidad	Acciones clave	Métricas/KPI
Gobernanza del SGSI	**Definir políticas**, revisar el alcance, alinear con la estrategia	**Revisiones ejecutivas**, % cumplimiento de políticas
Gestión de riesgos	**Identificar riesgos**, evaluación y planes de tratamiento	**Riesgos residuales**, % de riesgos mitigados
Respuesta a incidentes	**Plan de incidentes**, simulacros, coordinación con SOC	**MTTR**, número de incidentes críticos
Conformidad y auditoría	**Preparación para auditorías**, evidencias y seguimiento de no conformidades	**Estado de no conformidades**, tiempo de cierre
Concienciación y cultura	**Formación**, campañas y métricas de phishing	**Tasa de clics**, % de empleados formados

GESTION DE LA COMUNICACIÓN Y DOCUMENTACION

PLAN DE COMUNICACIÓN ISO 27001

La norma **ISO 27001** incluye requisitos en relación a la comunicación de la política de seguridad en una empresa. Se nos pide dar una respuesta a:

- Quien debe comunicar los aspectos de seguridad
- A quienes debe llegar la comunicación
- Cuál es el contenido
- En qué momento ha de realizarse la comunicación
- Que medios utilizaremos

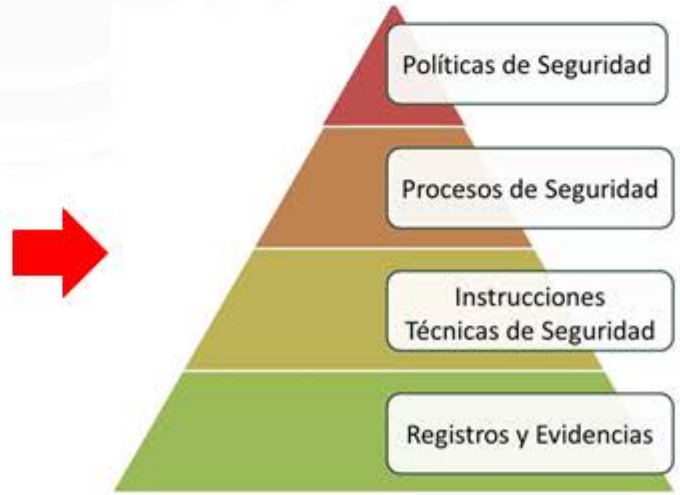
¿QUÉ INFORMACIÓN DEBE PUBLICARSE?

La información oficial del sistema SGI debería estar disponible para el personal que tenga derecho a su consulta.

En cuanto al medio de publicación no tenemos ningún requisito específico en la norma sin embargo, resulta conveniente que se publique en soportes electrónicos y que faciliten su difusión tales como intranet o en entornos de red compartidos

Los requisitos de la norma ISO 27001 en este caso nos piden que la documentación:

- Este completa
- Se encuentre actualizada
- Se realice un control de la documentación. Para ello lo más conveniente es tener un control mediante codificación que nos informe de la versión actualizada del documento y de las últimas modificaciones



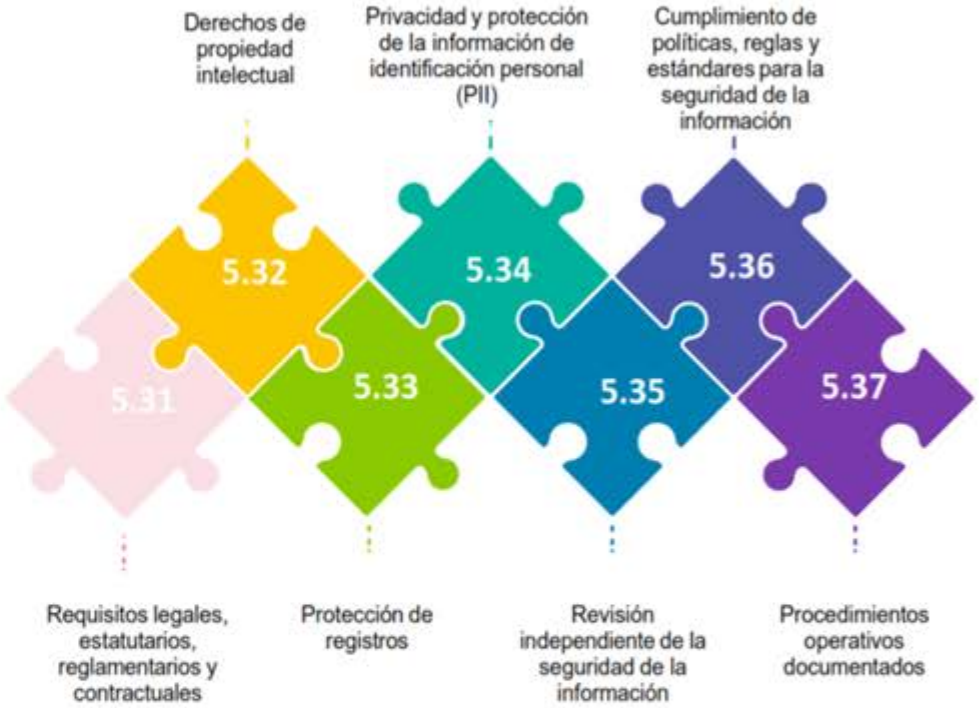
GESTION DE OPERACIONES

GESTION DE OPERACIONES

Controles Organizativos

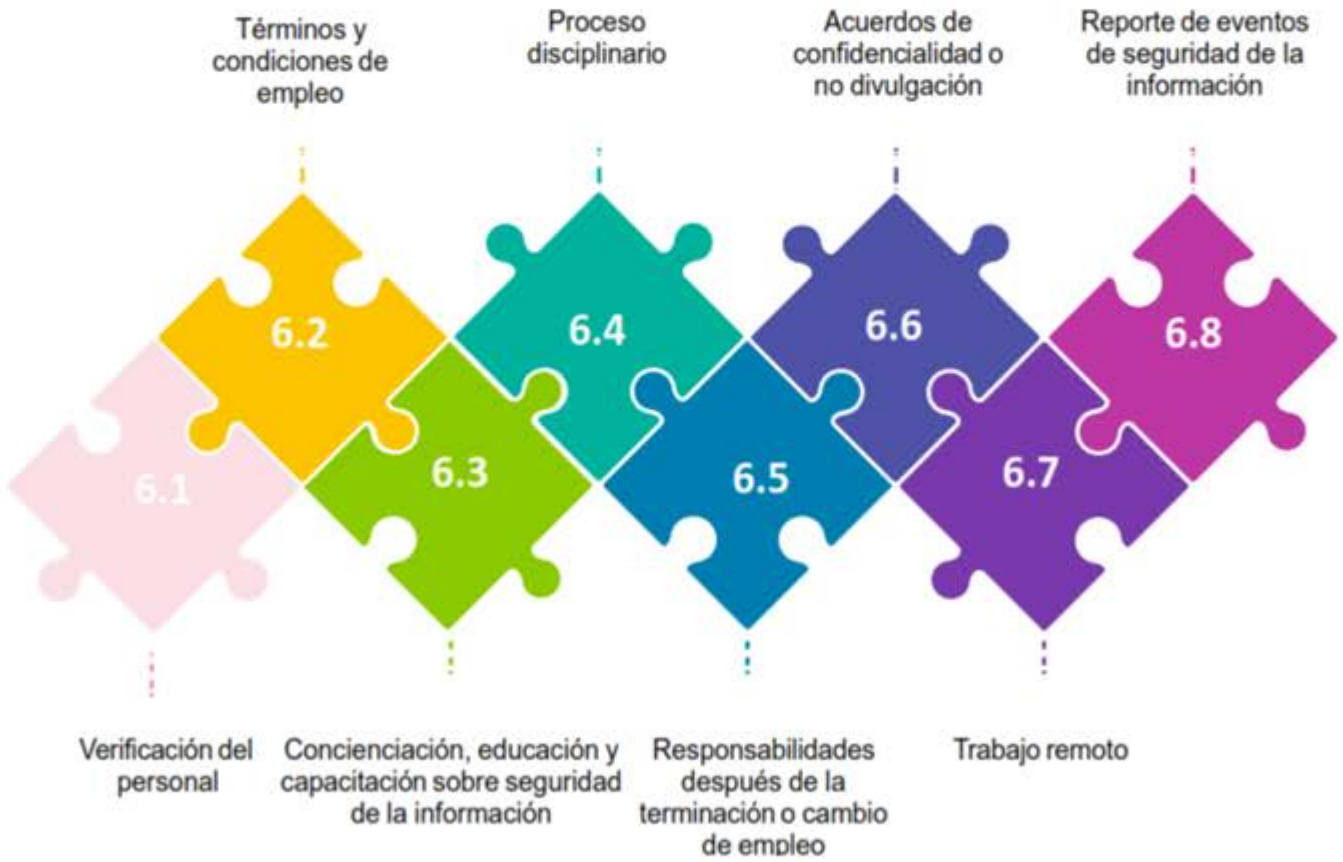
GESTION DE OPERACIONES

Controles Organizativos



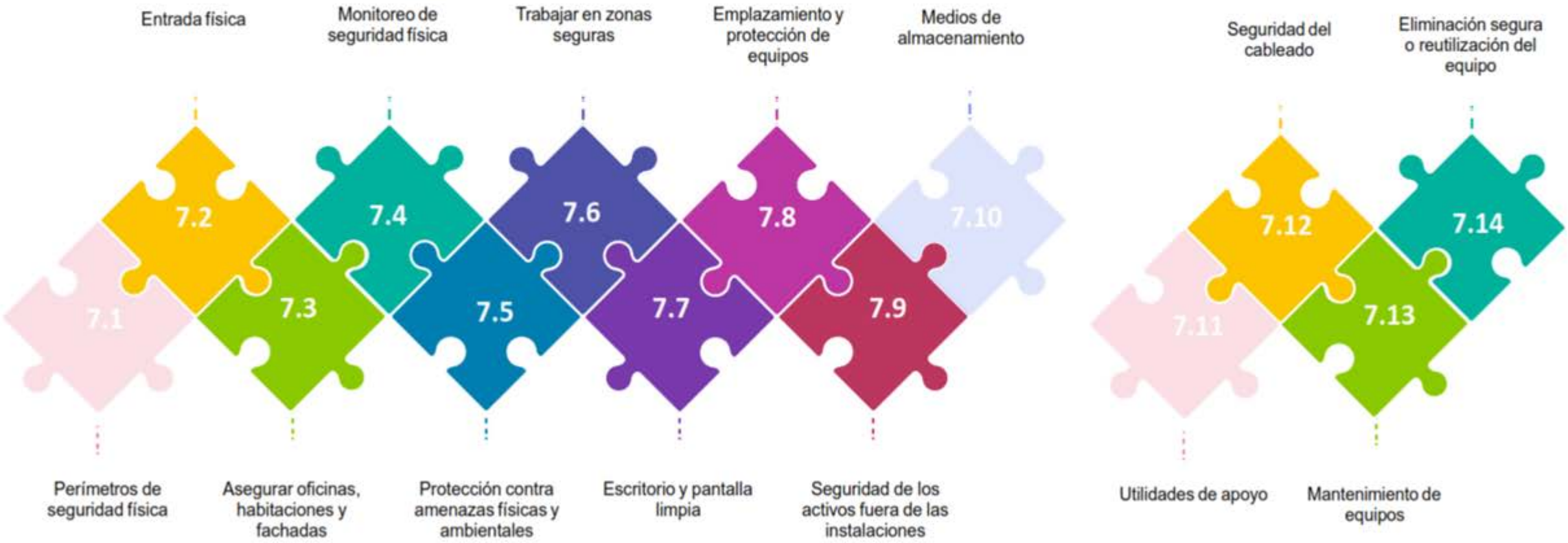
GESTION DE OPERACIONES

Controles de Personas



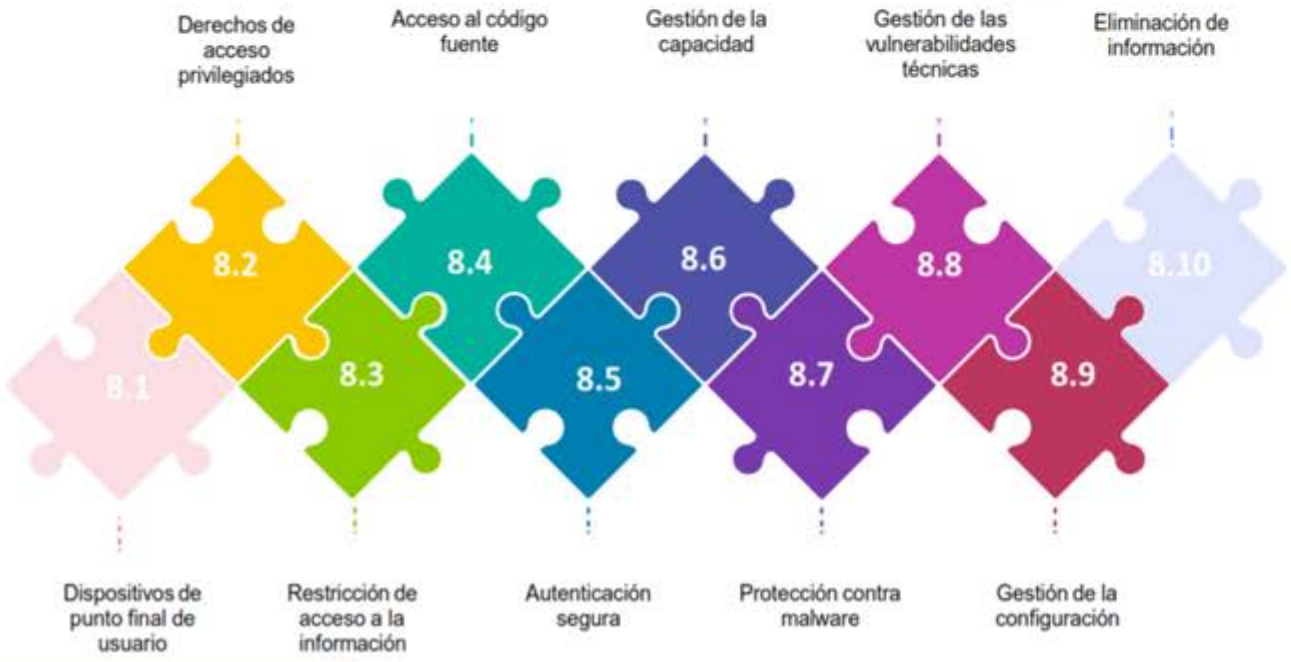
GESTION DE OPERACIONES

Controles Físicos



GESTION DE OPERACIONES

Controles Físicos



GESTION DE OPERACIONES

Controles Físicos

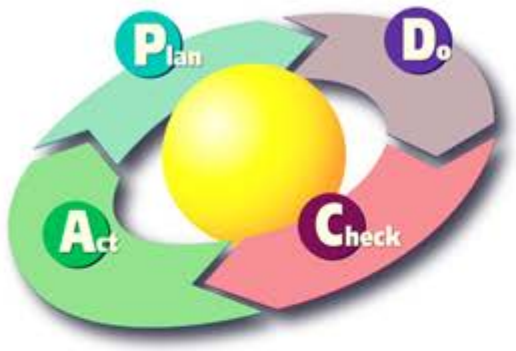
GESTIÓN DE LOS RIESGOS OPERACIONALES

4 Evaluar riesgos y su tratamiento

EVALUAR EL DESEMPEÑO

7 Evaluar el desempeño

MEJORA CONTINUA



8 Mejora Continua

- Definir **política de seguridad**
- Establecer **alcance del SGSI**
- Realizar **análisis de riesgos**
- Seleccionar los controles

P

- Implantar plan de **gestión de riesgos**
- Implantar el SGSI
- Implantar los **controles**
- **Formación y Concienciación**

ISO/IEC 27002 / Anexo A. ISO/IEC 27001

A

A5	Política de Seguridad de Información
A6	Organización de la Seguridad de la Información
A7	Seguridad en los RRHH
A8	Gestión de Activos
A9	Control de Accesos
A10	Criptografía
A11	Seguridad física y ambiental
A12	Seguridad en las operaciones

A.13	Seguridad en las comunicaciones
A.14	Adquisición, desarrollo y mantenimiento de sistemas
A15	Relación con proveedores
A16	Gestión de incidentes de seguridad
A17	Aspectos de Seguridad de la información dentro de continuidad de negocio
A18	Conformidad

D

- Adoptar las **acciones correctivas**
- Adoptar las acciones preventivas

C

- Revisar internamente el SGSI
- Realizar **auditorías internas** del SGSI
- Indicadores y Métricas
- Revisión por Dirección

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón