Formulario para el Sistema de Gestión Integral

# ¿Qué tipo de vulnerabilidades ha encontrado en el sistema de gestión integral respecto con los estándares de seguridad?

* 1. Las credenciales son predeterminadas
  2. Falta de políticas de permisos y accesos
  3. Sesiones sin control de tiempo

# ¿Qué tipos de pérdida de datos pueden ocurrir si el sistema ha sido comprometido por terceros y cómo afecta al cumplimiento de los estándares de seguridad de la información?

* 1. Pérdida de datos confidenciales (datos financieros, clientes)
  2. Pérdida de integridad de los datos (Modificaciones no autorizadas)
  3. Pérdida de disponibilidad de los datos (no existe un plan de respaldo)

1. ¿Qué tan clara es la política de la empresa respecto a la seguridad y manejo de datos de los clientes?
2. ¿Considera que el sistema de gestión integral cuenta con mecanismos adecuados para monitorear en tiempo real las actividades sospechosas y accesos no autorizados?
3. ¿El sistema de monitoreo está configurado para enviar alertas en caso de problemas de disponibilidad?
   1. No, el sistema no alerta a los clientes o usuarios si hay una caída prolongada
   2. Sí, el sistema envía SMS y notificaciones a los usuarios del aplicativo

# ¿Qué deficiencias presenta el sistema, respecto a la integridad de la información del inventario?

* 1. Inconsistencia entre el stock real y el stock virtual
  2. Falta de políticas de actualización de datos
  3. Cuando se realiza una compra, no se actualiza el stock

# ¿Qué deficiencias presenta el sistema en la integración de la información entre las áreas de almacén, logística y finanzas, según los estándares de auditoría de sistemas de información?

* 1. Identificación de falta de interoperabilidad
  2. El sistema no actualiza la información en tiempo real
  3. Falta de validación cruzada de datos entre áreas
  4. Ausencia de un control centralizado

# ¿Se realizan copias de seguridad periódicas de los datos y cómo se aseguran de que puedan ser restauradas rápidamente?

* 1. Diarias
  2. Semanales
  3. Mensuales

# ¿Ha percibido mejoras en la precisión de los reportes generados por el sistema tras la implementación de medidas correctivas identificadas en auditorías previas?

* 1. Si, los reportes muestran con gran precisión el stock y las transacciones correctas.
  2. No, los reportes no son claros ni concisos debido a que los datos han sido alterados.

# ¿Qué controles existen para garantizar que los datos críticos no sean modificados sin autorización?

* 1. Políticas de Control de Cambios
  2. Evaluaciones Mensuales
  3. Monitoreo y alertas en tiempo real

# accesos no autorizados a los sistemas de la empresa?

1. Muy efectivos, los controles cumplen con su propósito sin inconvenientes.
2. Bastante efectivos, aunque podrían reforzarse en algunas áreas.
3. Moderadamente efectivos, presentan vulnerabilidades ocasionales.
4. Poco efectivos, existen múltiples brechas de seguridad.
5. No efectivos, los accesos no autorizados son frecuentes.

# En su opinión, ¿en qué ayudaría integrar la información entre las áreas de almacén, logística y finanzas?

1. ¿Crees que el sistema garantiza una protección adecuada de la información confidencial de los clientes?
   1. Sí, totalmente
   2. En parte, hay riesgos asociados
   3. No presenta riesgos asociados

# ¿Consideras que el sistema cumple con los estándares de seguridad necesarios?

* 1. Sí completamente
  2. No cumple falta regularizar los estándares

# datos es suficiente para evitar perdida de datos?

1. Sí, totalmente suficiente.
2. Algo suficiente, pero podría mejorar.
3. Insuficiente, necesita ser reforzada.
4. No he recibido capacitación sobre este tema.

# ¿Los sistemas críticos de la empresa presentan caídas frecuentes?

* 1. Sí, ocurre constantemente (varias veces por semana).
  2. Ocasionalmente (una vez al mes o menos).
  3. Raramente (unas pocas veces al año).
  4. Nunca han presentado caídas.

# ¿Consideras que el personal es consciente y sigue las políticas de la empresa?

* 1. Sí, la mayoría sigue las políticas de ISO 27001
  2. Algunos las siguen, pero no todos.
  3. Muy pocos son conscientes de las políticas.
  4. No, el personal no sigue las políticas.

# el último año?

1. Sí, hubo intentos, pero se detectaron y gestionaron.
2. Sí, hubo intentos exitosos de acceso no autorizado.
3. No, no he notado intentos de acceso no autorizado.
4. No tengo conocimiento sobre este tema.

# ¿Con qué frecuencia cambia su contraseña?

* 1. Cada 1-3 meses.
  2. Cada 4-6 meses.
  3. Una vez al año.
  4. Solo cuando me lo solicitan.
  5. Nunca cambio mi contraseña.

# ¿Qué hallazgos ha identificado la auditoría interna que podrían comprometer la precisión de los registros de inventario?

Este contenido no ha sido creado ni aprobado por Google.

[](https://www.google.com/forms/about/?utm_source=product&utm_medium=forms_logo&utm_campaign=forms) [Formularios](https://www.google.com/forms/about/?utm_source=product&utm_medium=forms_logo&utm_campaign=forms)