ANEXO TECNICO CONTROLES POR CATEGORIA SEGÚN ISO/IEC-27001, versión 2022

Anexo A de la norma ISO/IEC 27001:2022, clasificados por las cuatro categorías introducidas en esta versión: *Controles Organizativos, Controles de Personas, Controles Físicos y Controles Tecnológicos*. Esta clasificación se corresponde con la estructura de ISO/IEC 27002:2022, de la cual ISO/IEC 27001:2022 deriva sus controles.

CONTROLES ORGANIZATIVOS (37 controles)

1. Políticas para la seguridad de la información
2. Roles y responsabilidades en seguridad de la información
3. Segregación de funciones
4. Gestión de conflictos de intereses
5. Contacto con las autoridades
6. Contacto con grupos de interés especializados
7. Inteligencia de amenazas
8. Seguridad de la información en la gestión de proyectos
9. Inventario de información y otros activos asociados
10. Uso aceptable de la información y activos asociados
11. Eliminación de la información
12. Clasificación de la información
13. Etiquetado de la información
14. Transferencia de la información
15. Control de acceso
16. Gestión de identidades
17. Información de autenticación (gestión de credenciales)
18. Derechos de acceso
19. Seguridad de la información en las relaciones con proveedores
20. Seguridad de la información en los acuerdos con proveedores
21. Gestión de la seguridad de la información en la cadena de suministro
22. Monitoreo, revisión y evaluación de servicios de terceros
23. Seguridad de la información en relaciones con organizaciones colaboradoras
24. Gestión de la seguridad de la información en entornos interconectados
25. Ciclo de vida de desarrollo seguro
26. Procesos seguros de desarrollo y soporte
27. Desarrollo externalizado
28. Datos de prueba
29. Eliminación segura o reutilización de equipos
30. Soportes físicos en tránsito
31. Liberación segura de código
32. Gestión de vulnerabilidades técnicas
33. Continuidad de la seguridad de la información
34. Redundancias
35. Registro (logging)
36. Sincronización de relojes
37. Información de eventos

CONTROLES DE PERSONAS (8 controles)

1. Verificación de antecedentes del personal
2. Responsabilidades en materia de seguridad de la información durante el empleo

3. Capacitación, concienciación y formación en seguridad de la información
4. Gestión del personal al finalizar o cambiar su relación laboral
5. Canal de denuncia (whistleblowing)
6. Responsabilidades en el trabajo remoto
7. Protección del personal en entornos hostiles
8. Viajes seguros

CONTROLES FÍSICOS (14 controles)

1. Perímetro físico seguro
2. Controles físicos de acceso
3. Protección contra amenazas físicas y ambientales
4. Áreas seguras de trabajo
5. Suministro seguro de servicios públicos
6. Ubicación y protección del equipo
7. Seguridad del cableado
8. Mantenimiento del equipo
9. Eliminación segura del equipo con información
10. Protección contra interrupciones eléctricas y fallos del sistema
11. Segregación física de la información crítica
12. Protección de activos fuera de las instalaciones
13. Medios de almacenamiento transportables seguros
14. Recepción y envío seguro de la información

CONTROLES TECNOLÓGICOS (34 controles)

1. Gestión del control de acceso lógico a sistemas e información
2. Autenticación y gestión de credenciales
3. Principio del privilegio mínimo en el acceso
4. Eliminación o deshabilitación de cuentas no necesarias
5. Restricciones sobre el software instalado por el usuario
6. Protección contra software malicioso
7. Copias de seguridad (backups) a nivel tecnológico
8. Registro de eventos y monitoreo de sistemas
9. Detección de anomalías
10. Seguridad de las redes
11. Control de acceso a redes y conexiones remotas
12. Seguridad de servicios en la nube
13. Seguridad de las comunicaciones
14. Seguridad del correo electrónico y mensajería
15. Protección de la información en tránsito
16. Protección de la información en reposo
17. Cifrado
18. Gestión de claves criptográficas
19. Integridad del software y las plataformas
20. Desarrollo seguro de software
21. Pruebas de seguridad del software
22. Gestión de la configuración segura
23. Gestión de vulnerabilidades técnicas
24. Monitoreo de la seguridad tecnológica
25. Respuesta a incidentes tecnológicos

26. Gestión de la capacidad y disponibilidad tecnológica
27. Protección contra ataques de denegación de servicio
28. Segregación lógica en entornos multiusuario
29. Seguridad en entornos virtualizados y contenedores
30. Seguridad de dispositivos móviles
31. Seguridad de Internet de las cosas (IoT)
32. Prevención de fuga de datos (DLP)
33. Control del uso indebido de servicios basados en información
34. Seguridad en sistemas de control industrial (ICS)

Anexo, Política de Control de Accesos.

A continuación, se presenta un modelo de política basado en los lineamientos de ISO 27001, de tal forma que la CAS Santander, pueda formalizar dicha política dentro del modelo de Seguridad y Privacidad de la información, MSPI, y materializarla en el sistema de gestión de seguridad de la información. Es recomendable que cada numeral que implica acción ir avanzando paso a paso en su implementación. Debe estar coordinada y gestionada por el Oficial de Seguridad que defina la CAS Santander.

1. Propósito

El objetivo de esta política es establecer los lineamientos necesarios para gestionar y controlar el acceso a los sistemas de información, recursos tecnológicos, y datos sensibles de la entidad, asegurando la protección de la confidencialidad, integridad y disponibilidad de la información, conforme a los requisitos de la norma ISO 27001 y la legislación aplicable.

2. Alcance

Esta política aplica a:

- Todos los empleados, contratistas, proveedores y terceros (comunidad) que accedan a los sistemas de información y recursos tecnológicos de la entidad.
- Todos los sistemas de información, bases de datos, aplicaciones, equipos, redes y otros activos tecnológicos.

3. Principios

1. **Acceso basado en necesidad y rol (Least Privilege):** El acceso a la información y sistemas estará restringido a las personas autorizadas en función de sus responsabilidades laborales y solo al nivel mínimo requerido.
2. **Autenticación robusta:** Todos los accesos deberán estar protegidos mediante métodos de autenticación seguros, como contraseñas fuertes o autenticación multifactor (MFA).
3. **Revisión periódica:** Los permisos y roles serán revisados periódicamente para asegurar que continúen siendo necesarios y apropiados.
4. **Registros de auditoría:** Todas las actividades de acceso serán registradas y monitoreadas para identificar posibles accesos no autorizados o actividades sospechosas.

4. Directrices

4.1. Gestión de Cuentas de Usuario

1. Todas las cuentas de usuario deberán ser creadas, modificadas o eliminadas exclusivamente por el área de TI mediante una solicitud documentada y aprobada.
2. Las cuentas de usuario deben estar asociadas a un individuo específico. No se permite el uso de cuentas genéricas o compartidas, salvo que sea estrictamente necesario y aprobado.
3. Las contraseñas deberán cumplir con los siguientes requisitos:
    - Longitud mínima de 12 caracteres.
    - Inclusión de letras mayúsculas, minúsculas, números y caracteres especiales.

- Cambio obligatorio cada 90 días.
- Prohibición de reutilizar las últimas 5 contraseñas.

4.2. Autenticación Multifactor (MFA)

1. El uso de MFA es obligatorio para:
   - Acceso a sistemas críticos.
   - Acceso remoto a la red corporativa.
2. Los métodos aceptables de MFA incluyen:
   - Aplicaciones de autenticación (Google Authenticator, Microsoft Authenticator).
   - Tokens físicos o virtuales.
   - Biometría.

4.3. Control de Accesos Físicos

1. El acceso a áreas restringidas, como los centros de datos, estará limitado a personal autorizado.
2. Se implementarán controles físicos como cerraduras electrónicas, tarjetas de acceso y registro de visitantes.
3. Todo acceso a áreas restringidas deberá ser registrado y auditado periódicamente.

4.4. Revisión de Accesos

1. Los permisos de acceso serán revisados trimestralmente por los responsables de área y el área de TI.
2. El acceso de empleados que cambien de rol o dejen la organización deberá ser revocado dentro de las 24 horas siguientes al cambio.
3. Las cuentas inactivas por más de 30 días serán deshabilitadas automáticamente.

4.5. Monitoreo y Registro de Accesos

1. Todas las actividades de acceso deberán ser registradas mediante herramientas de monitoreo.
2. Los registros incluirán:
   - Fecha, hora y ubicación del acceso.
   - Identidad del usuario.
   - Recursos accedidos.

   Los registros serán revisados mensualmente para identificar patrones sospechosos.

5. Roles y Responsabilidades

1. **Área de TI:**
   - Implementar y gestionar los controles definidos en esta política.
   - Revisar periódicamente los permisos de acceso.
   - Responder a incidentes relacionados con accesos no autorizados.

2. **Responsables de área:**

    - Autorizar y validar los accesos solicitados por sus colaboradores.
    - Informar cambios en el personal que requieran ajustes en los permisos.

3. **Usuarios finales:**

    - Respetar las políticas de acceso.
    - Reportar incidentes de seguridad relacionados con accesos.

6. Auditoría y Cumplimiento

1. Esta política será revisada anualmente para garantizar su vigencia y alineación con los objetivos de la organización.
2. El cumplimiento de esta política será auditado trimestralmente por el área de TI y el comité de seguridad.
3. Las violaciones a esta política podrán resultar en sanciones disciplinarias según las normativas de la organización.

7. Vigencia

Esta política entra en vigor a partir de su aprobación y será de obligatorio cumplimiento para todos los involucrados.

Aprobado por:

[Nombre y Cargo]
[Fecha]

Anexo, política de control de incidentes.

La gestión de la política de "Control de incidentes" relacionado con el MSPI debe implementarse en proceso y procedimientos formales que en lo posible cuenten con una herramienta informática que facilite su gestión y trazabilidad. En el PETI 2025-2027, se identifica un proyecto que busca a través de la intranet establecer los flujos de trabajo que permitan el registro y la debida gestión. A continuación, se presenta un modelo de política a implementar.

1. Propósito

Esta política establece los lineamientos para la identificación, registro, investigación, gestión y resolución de incidentes de seguridad de la información en la entidad. Su objetivo es minimizar el impacto de los incidentes en las operaciones, proteger los activos de información y garantizar la mejora continua en la gestión de la seguridad.

2. Alcance

Esta política aplica a:

- Todos los empleados, contratistas y terceros que accedan a los sistemas de información de la entidad.
- Todos los sistemas, aplicaciones, redes y activos tecnológicos.
- Cualquier incidente relacionado con la confidencialidad, integridad, disponibilidad o privacidad de la información.

3. Definiciones

- **Incidente de Seguridad:** Evento o serie de eventos inesperados que comprometen o pueden comprometer la seguridad de la información.
- **Evento de Seguridad:** Cualquier acción que puede ser relevante para la seguridad pero que no necesariamente representa un incidente.
- **CSIRT:** Equipo de Respuesta a Incidentes de Seguridad Informática, responsable de gestionar los incidentes.

4. Principios

1. **Detección temprana:** Los incidentes deben ser identificados lo más pronto posible para reducir su impacto.
2. **Registro y trazabilidad:** Todos los incidentes deben ser documentados de forma completa y precisa.
3. **Respuesta coordinada:** Los incidentes deben ser gestionados de manera estructurada y con roles definidos.
4. **Mejora continua:** Los aprendizajes derivados de los incidentes deben ser utilizados para fortalecer los controles de seguridad.

5. Directrices

5.1. Notificación de Incidentes

1. Todos los usuarios deben reportar incidentes de seguridad tan pronto como sean detectados utilizando los canales definidos por la entidad (correo electrónico, teléfono o portal de reportes).
2. Los incidentes críticos deben ser escalados inmediatamente al CSIRT.

5.2. Clasificación de Incidentes

Los incidentes se clasificarán según:

- **Impacto:** Bajo, medio, alto.
- **Urgencia:** Inmediata, prioritaria, normal.

5.3. Respuesta a Incidentes

1. El CSIRT (Computer Security Incident Response Team, equipo encargado de gestionar los incidentes de seguridad de la información) iniciará una investigación para determinar:
    - La causa del incidente.
    - Los sistemas o datos afectados.
    - Las medidas correctivas necesarias.
2. Dependiendo de la severidad, se activará el plan de contingencia o de recuperación.
3. Las acciones inmediatas incluirán:
    - Contención del incidente para evitar mayores daños.
    - Eliminación de las causas del incidente.
    - Restauración de los servicios afectados.

5.4. Registro y Documentación

1. Todos los incidentes deben ser registrados en un sistema de gestión de incidentes, incluyendo:
    - Fecha y hora del incidente.
    - Descripción del incidente.
    - Acciones realizadas y resultados.
2. El registro debe incluir evidencias relevantes (logs, capturas de pantalla, archivos afectados).

5.5. Análisis Post-Incidente

1. Una vez resuelto el incidente, se realizará un análisis para:
    - Identificar la causa raíz.
    - Proponer mejoras para evitar incidentes similares.
    - Evaluar la efectividad de la respuesta.
2. Se documentará un informe post-incidente que será revisado por el Comité de Seguridad de la Información.

5.6. Comunicación de Incidentes

1. Los incidentes relevantes serán comunicados a las partes interesadas internas y externas según corresponda.

2. En caso de incidentes graves que afecten datos personales, se notificará a la Superintendencia de Industria y Comercio en los términos establecidos por la ley.

5. Roles y Responsabilidades

1. **Usuarios finales:**
   - Reportar cualquier incidente de seguridad detectado.
2. **CSIRT:**
   - Gestionar los incidentes de seguridad según los procedimientos establecidos.
   - Proveer informes de incidentes a la dirección y partes interesadas.
3. **Área de TI:**
   - Implementar controles preventivos y correctivos derivados de los incidentes.
4. **Comité de Seguridad de la Información:**
   - Revisar los informes post-incidente y recomendar mejoras.

6. Auditoría y Cumplimiento

1. Esta política será revisada anualmente para garantizar su alineación con los objetivos organizacionales.
2. El cumplimiento de esta política será auditado trimestralmente.
3. Las desviaciones o incumplimientos serán reportados y tratados mediante acciones correctivas.

Vigencia

Esta política entra en vigor a partir de su aprobación y es de cumplimiento obligatorio para todos los involucrados.

Aprobado por:

[Nombre y Cargo]

[Fecha]

Anexo, Política para la Gestión de Copias de Seguridad

1. Propósito

El objetivo de esta política es establecer un marco para la creación, almacenamiento, protección y recuperación de copias de seguridad de la información crítica de la entidad. Esta política garantiza la continuidad de las operaciones en caso de pérdida de datos, desastres, o fallos en los sistemas de información, alineándose con los requisitos de la norma ISO 27001.

2. Alcance

Esta política aplica a:

- Toda la información crítica almacenada en sistemas, bases de datos y dispositivos de la entidad.
- Los empleados, contratistas y terceros responsables de la gestión y mantenimiento de sistemas de información.
- Todos los sistemas y medios utilizados para realizar copias de seguridad.

3. Principios

1. **Confidencialidad:** Las copias de seguridad deben protegerse contra accesos no autorizados.
2. **Integridad:** Garantizar que las copias de seguridad sean fidedignas y libres de corrupción.
3. **Disponibilidad:** Asegurar que las copias de seguridad estén disponibles para su restauración en caso necesario.
4. **Periodicidad:** Establecer un calendario regular para la realización de copias de seguridad.

4. Directrices

4.1. Identificación de Información Crítica

1. La información crítica será identificada y clasificada por cada área de la entidad en coordinación con el área de TI.
2. Los sistemas, aplicaciones y bases de datos que contengan información crítica deberán estar documentados.

4.2. Creación de Copias de Seguridad

1. Las copias de seguridad deberán realizarse según el siguiente calendario:
    - **Diarias:** Para datos críticos y transaccionales.
    - **Semanales:** Para configuraciones y datos secundarios.
    - **Mensuales:** Para datos de archivo y respaldo a largo plazo.
2. Las copias de seguridad deben incluir:
    - Datos críticos.
    - Configuraciones de sistemas.
    - Registros de auditoría relevantes.
3. Se debe validar la completitud y exactitud de cada copia mediante verificaciones automáticas y manuales.

4.3. Almacenamiento de Copias de Seguridad

1. Las copias de seguridad se almacenarán en:
    - Ubicaciones locales seguras (on-premise).
    - Ubicaciones remotas o en la nube para redundancia.
2. Todas las copias deben ser cifradas utilizando algoritmos robustos (AES-256 o superior).
3. Se implementará un control de acceso estricto para el almacenamiento de las copias de seguridad.
4. Las copias de seguridad se conservarán según el siguiente esquema:
    - **Diarias:** 7 días.
    - **Semanales:** 1 mes.
    - **Mensuales:** 1 año o según normativas aplicables.

4.4. Pruebas de Restauración

1. Las pruebas de restauración se realizarán:
    - Al menos trimestralmente para garantizar la efectividad de las copias.
    - Siempre que se introduzcan cambios significativos en los sistemas.
2. Todas las pruebas deberán documentarse, incluyendo resultados y acciones correctivas.

4.5. Monitoreo y Registro

1. Todas las actividades relacionadas con las copias de seguridad serán registradas en un sistema de gestión.
2. Los registros incluirán:
    - Fecha y hora de la copia.
    - Datos respaldados.
    - Responsable de la operación.
    - Resultado de la operación (exitoso o fallido).

5. Roles y Responsabilidades

1. **Área de TI:**
    - Configurar y supervisar las copias de seguridad.
    - Realizar pruebas periódicas de restauración.
    - Gestionar el almacenamiento y seguridad de las copias.
2. **Responsables de área:**
    - Identificar y comunicar información crítica.
    - Coordinar con el área de TI para asegurar el cumplimiento de esta política.
3. **Usuarios finales:**
    - Reportar datos que requieran respaldo inmediato.

6. Auditoría y Cumplimiento

1. Esta política será revisada anualmente para garantizar su vigencia.
2. Las auditorías periódicas validarán el cumplimiento de:
    - Calendarios de copia.
    - Pruebas de restauración.
    - Cifrado y almacenamiento seguro.
3. Las desviaciones serán reportadas al Comité de Seguridad de la Información.

7. Vigencia

Esta política entra en vigor a partir de su aprobación y es de cumplimiento obligatorio para todos los involucrados.

Aprobado por:

[Nombre y Cargo]

[Fecha]