POLÍTICA SEGURIDAD DE LA INFORMACIÓN

Autor: Consultor Organización: **ESTUDNET SL**	Validado por: Responsable de Seguridad de la Información Organización: **Cambridge Business Initiatives S.L.**	Aprobado por: Comité de Seguridad Organización: **Cambridge Business Initiatives S.L.**
Fecha: 07/03/2024	**Fecha:** 09/08/2024	**Fecha**: 09/08/2024
Documento: Política de Seguridad 27001		
Descripción: La alta dirección debe establecer una política de seguridad de la información que: a) sea adecuada al propósito de la organización; b) incluya objetivos de seguridad de la información o proporcione un marco de referencia para el establecimiento de los objetivos de seguridad de la información; c) incluya el compromiso de cumplir con los requisitos aplicables a la seguridad de la información; e d) incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información. La política de seguridad de la información debe: e) estar disponible como información documentada; f) comunicarse dentro de la organización; y g) estar disponible para las partes interesadas, según sea apropiado		

DECLARACIÓN

(texto público a difundir a terceras partes: clientes, proveedores, reguladores, ciudadanía)

Cambridge Business Initiatives S.L. (en adelante, **SYGRIS**) es la creadora de una plataforma que digitaliza la gestión de datos y procesos no financieros, enfocada en sostenibilidad y cumplimiento de normativas ESG. Sus servicios incluyen el reporte de información no financiera, gestión de planes de sostenibilidad, cálculo de huella de carbono, y gestión de residuos. Además, abarcan áreas sociales como la gestión de voluntariado, recursos humanos, y salud y seguridad. En gobernanza, Sygris ofrece herramientas para la gestión de riesgos, auditorías, y acreditación de proveedores.

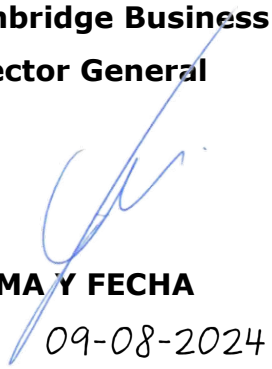
La dirección de **SYGRIS,** consciente de la importancia de la ciberseguridad ha establecido la organización, los procesos, las herramientas y los controles para garantizar la confidencialidad, la integridad, la autenticidad y la trazabilidad de la información, así como de la disponibilidad de los servicios que se prestan a los clientes, de conformidad con los estándares internacionales, con los siguientes **objetivos**:

- Concienciar y formar al personal en seguridad y privacidad de la información.
- Evaluar y tratar los riesgos de la seguridad y privacidad de la información.
- Prevenir y responder eficazmente ante eventos o incidentes de seguridad de la información.
- Garantizar la continuidad de las operaciones de negocio.
- Cumplir proactivamente la legislación de protección de datos personales, de propiedad intelectual e industrial y cualquier otra aplicable.
- Evaluar la eficacia y eficiencia de los procesos y los controles de seguridad de la información.
- Mejorar continuamente la gestión de la seguridad de la información.

La Dirección del **SYGRIS**, en consecuencia, con todo lo anterior, está comprometida con la asignación de recursos humanos y materiales, necesarios y proporcionados para el logro de los anteriores objetivos.

La supervisión de la seguridad de la información la asume la Dirección de **SYGRIS**, delegando en el **Responsable de Seguridad de la Información** las competencias para la implantación y certificación de un Sistema de Gestión de Seguridad y de la Información (SGSI), contando con el respaldo de todo su equipo humano y de colaboradores.

Cambridge Business Initiatives S.L.
Director General



FIRMA Y FECHA
09-08-2024

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

(texto de difusión controlada a clientes, proveedores, reguladores)

Para el cumplimiento de la presente Política de Seguridad de la Información de **Cambridge Business Initiatives S.L. (en adelante, SYGRIS)** dispone de un sistema de gestión de seguridad de la información (en adelante, SGSI), de conformidad con estándares internacionales, que da cobertura a los requisitos necesarios para garantizar la confidencialidad, la integridad, la autenticidad y la trazabilidad de la información, así como de la disponibilidad de los servicios que se prestan a los clientes.

Para la eficacia y eficiencia del sistema de gestión de seguridad de la información, la Dirección de SYGRIS ha tomado las decisiones siguientes:

1. Adoptar los estándares ISO/IEC 27001 como marco normativo del SGSI.
2. Asignar los recursos de talento y medios materiales para el desarrollo del ciclo de vida del SGSI.
3. Designar un responsable de seguridad de la información, con la autoridad delegada para el desarrollo, mantenimiento y mejora del SGSI.
4. Establecer la organización, con una definición clara de roles y responsabilidades, para la gestión de seguridad de la información.
5. Planificar la formación y concienciación del personal y colaboradores para saber actuar preventivamente y reaccionar, en su caso, ante las amenazas a la seguridad de la información.
6. Analizar los riesgos a la seguridad de la información como proceso esencial para prevenir los incidentes de seguridad de la información.
7. Cumplir proactivamente los requisitos legales, normativos y reglamentarios aplicables.
8. Medir y analizar los indicadores que permitan a la Dirección el seguimiento de los objetivos de seguridad.
9. Monitorizar, revisar y auditar regularmente el SGSI.

En consecuencia con lo anterior, la Dirección de **SYGRIS** ha establecido las políticas que, a continuación, se resumen.

1. **La seguridad de la información es responsabilidad de todos**

La Dirección supervisará las medidas de seguridad de la información, siendo su observancia responsabilidad de todo el personal y colaboradores.

La Dirección aportará los medios necesarios y proporcionales, de acuerdo con un modelo de mejora continua, con especial énfasis en la formación de los recursos humanos, así como el control y análisis de los resultados para verificar la eficiencia y eficacia de las medidas.

2. **La gestión proactiva de ciber-riesgos**

Para gestionar los riesgos derivados de las amenazas a los activos de información se seguirán las siguientes medidas:

- La asignación de los recursos especializados necesarios para la realización del análisis de riesgos.
- Registrar los análisis de riesgo realizados y someter la aceptación del nivel de riesgo residual a la aprobación de la Dirección General.
- Establecer un valor objetivo de puntuación media máxima, identificándose asimismo un valor inadmisible de riesgo y un rango como intervalo tolerable.
- El Responsable de Seguridad de la Información de **SYGRIS** actualizará el análisis de riesgos con periodicidad semestral o, bien, cuando ocurra un incidente relevante, estableciendo las medidas para su debido tratamiento.

3. **Protección de los dispositivos, los aplicativos y las comunicaciones.**

Para garantizar el uso aceptable de los dispositivos y aplicativos, que **SYGRIS** pone a disposición de los usuarios de sus sistemas de información, se seguirán las siguientes medidas:

- Los dispositivos son propiedad de **SYGRIS** puestos a disposición de los usuarios únicamente para su desempeño laboral.
- La instalación y uso de cualquier aplicativo, programa software o contenido digital, ajeno a los instalados o autorizados, está terminantemente prohibido. Tampoco se admitirán modificaciones a los elementos del hardware de los dispositivos de **SYGRIS**.
- Todos los aplicativos o programas software instalados en los dispositivos de **SYGRIS** deberán cumplir con el modelo de licenciamiento de sus fabricantes.

4. Control del acceso físico

Para garantizar el debido acceso a oficinas e instalaciones de **SYGRIS**, se siguieron las siguientes medidas:

- La entrada y salida a las oficinas e instalaciones de personas no pertenecientes a la organización serán autorizadas por un responsable y registradas en la recepción.
- Las personas autorizadas no pertenecientes a la organización que accedan a las zonas donde se ubiquen dispositivos y/o equipos de comunicaciones estarán supervisadas por un responsable.

5. Protección de infraestructuras e instalaciones

Para garantizar la protección de infraestructuras e instalaciones de **SYGRIS** se seguirán las siguientes medidas:

- El suministro eléctrico a los sistemas de información en caso de fallo del suministro general.
- La instalación de medios de detección y extinción de incendios.
- La instalación de medios de detección de intrusiones.
- La protección, mediante canalizaciones, de incidentes fortuitos o deliberados, del cableado de redes de datos y voz.
- La existencia de instalaciones alternativas para la continuidad de las operaciones en caso de que las instalaciones habituales no estén disponibles.

6. Control de acceso de los usuarios

Para garantizar el debido acceso a los dispositivos o programas software de **SYGRIS** se seguirán las siguientes medidas:

- A todo usuario se le asignará un nombre de usuario único y una contraseña, que tendrán carácter estrictamente personal e intransferible, otorgados en función de sus necesidades y autorización de acceso a la información.
- Las contraseñas iniciales serán configuradas por **SYGRIS**.
- Las contraseñas de los usuarios se renovarán cada 180 días.
- Las contraseñas de los usuarios con permisos de administración se renovarán cada 90 días.

- Los nombres de usuarios y contraseñas serán cambiadas o eliminadas cuando se produzca un cambio de funciones o baja, respectivamente o bien un incidente que haya comprometido su confidencialidad.

7. Control del uso de Internet

Para garantizar el acceso y uso aceptable de Internet por los usuarios se seguirán las siguientes medidas:

- El acceso y navegación por Internet de los usuarios estará monitorizado, registrándose la actividad realizada.
- La utilización de Internet, como herramienta de trabajo útil, se ajustará a las necesidades del desempeño laboral de cada usuario.
- El acceso de los usuarios a páginas inseguras o inapropiadas de Internet está prohibido de acuerdo con las prácticas reconocidas de buen uso y/o de conformidad con la legislación vigente.

8. Protección del correo electrónico

Para garantizar el uso aceptable del correo electrónico por los usuarios, se seguirán las siguientes medidas:

- Las cuentas de correo electrónico asignadas a los usuarios para el desempeño de sus actividades profesionales son propiedad de **SYGRIS**.
- Los contenidos de los correos electrónicos serán confidenciales ajustándose al ordenamiento legal.
- A todos los usuarios de las cuentas de correo electrónico se les asigna una dirección electrónica única y una contraseña, de carácter estrictamente personal e intransferible.
- Las contraseñas iniciales serán configuradas por **SYGRIS**.
- Las contraseñas de los usuarios se renovarán cada 180 días.
- Las contraseñas de los usuarios con permisos de administración se renovarán cada 90 días.

9. Filtrado de contenidos dañinos

Para garantizar la identificación, bloqueo y eliminación de contenidos dañinos, se seguirán las siguientes medidas:

- La instalación en los dispositivos de los usuarios de antivirus y antispam
- No desactivar nunca los programas antivirus y antispam.

- Reiniciar siempre el dispositivo para finalizar la instalación de las actualizaciones.

10. Protección de los sistemas operativos y otras utilidades

Para garantizar la eliminación de vulnerabilidades en los sistemas operativos y otras utilidades instaladas en los dispositivos de los usuarios, se seguirán las siguientes medidas:

- No desactivar nunca las herramientas de actualización.
- Reiniciar siempre el dispositivo para finalizar la instalación de las actualizaciones.

11. Protección de los dispositivos personales.

Para garantizar el uso aceptable de los dispositivos personales de los usuarios (BYOD) se seguirán las siguientes medidas:

- La autorización de los usuarios y dispositivos (teléfonos inteligentes, tabletas) para el uso de los servicios de correo electrónico, de conectividad a Internet y de los aplicativos de negocio.
- La instalación en los dispositivos personales de los usuarios de antivirus y antispam.
- La actualización del software del sistema operativo y otras utilidades del sistema de los dispositivos personales de los usuarios.
- La disposición en los dispositivos personales de los usuarios de clave o pin de acceso.
- Los aplicativos o programas software instalados en los dispositivos personales de los usuarios autorizados deberán contar con las licencias de uso y/o mantenimiento de sus fabricantes.
- La suscripción de un compromiso de uso aceptable por parte de los usuarios de los dispositivos personales autorizados para el acceso y uso de los servicios de correo electrónico, de conectividad a Internet y de los aplicativos de negocio.

12. Protección del teletrabajo o movilidad

Para garantizar la seguridad en situaciones de movilidad y/o teletrabajo se seguirán las siguientes medidas:

- La autorización de los usuarios y dispositivos en situaciones de movilidad y/o teletrabajo para el uso de los servicios de correo electrónico, de conectividad a Internet y/o de los aplicativos de negocio.
- La instalación en los dispositivos de los usuarios autorizados para situaciones de movilidad y/o teletrabajo del aplicativo para acceso remoto seguro (VPN) proporcionado por **SYGRIS**. No está permitido el uso de otros aplicativos de acceso seguro remoto.
- La utilización de doble factor de autenticación para la identificación de los usuarios del aplicativo para acceso remoto seguro (VPN).
- La renovación de la contraseña de acceso cada 90 días.
- La actualización puntual del software del aplicativo para el acceso remoto seguro (VPN) proporcionado por **SYGRIS**
- La habilitación de la protección de dispositivo desatendido mediante su bloqueo por inactividad.
- El uso de elementos de protección de dispositivos en movilidad y/o teletrabajo (mochila y candado de anclaje).
- La suscripción de un compromiso de uso aceptable por parte de los usuarios de los dispositivos autorizados para el acceso remoto seguro en movilidad y/o teletrabajo.

13. Protección de las comunicaciones.

Para garantizar la eliminación de vulnerabilidades en los servidores y equipos de electrónica de red (routers, switches, puntos de acceso, proxis) se seguirán las siguientes medidas:

- La actualización puntual del software de servidores y firmware de los equipos de la electrónica de red.
- La segregación lógica, mediante redes locales virtuales, de las redes no esenciales para la prestación del servicio a los clientes (redes wifi de invitados, de unidades de apoyo a negocio, etc.).
- La monitorización continúa de servidores y equipos de electrónica de red.

14. Copias de seguridad

Para garantizar la recuperación de los datos, en caso de pérdida, secuestro o destrucción, se seguirán las siguientes medidas:

- La información de los usuarios será objeto de la realización regular de copias de seguridad o respaldo (backup).
- Las copias de seguridad serán debidamente custodiadas y conservadas.
- Las copias de seguridad serán probadas regularmente para asegurar su recuperación.

15. Gestión de incidentes

Para garantizar la contención, mitigación y recuperación ante eventos desfavorables que puedan afectar a la seguridad y privacidad de la información y/o la disponibilidad de los servicios, se seguirán las siguientes medidas:

- La comunicación puntual por cualquier usuario de la observación de un evento sospechoso, tal como: pérdida de control de los dispositivos o aplicativos, desconexión súbita del sistema, recepción de un correo electrónico, SMS y/o llamada sospechosa, presencia de personas desconocidas no autorizadas en las oficinas o dependencias, etc.
    - La comunicación se realizará mediante la cuenta de correo security@sygris.com o por comunicación telefónica cuando se estime urgente.
- El registro, la evaluación y la notificación a los afectados y/o a las Autoridades, en su caso.
- La convocatoria del Comité de Crisis cuando la evaluación del incidente se estime de elevada peligrosidad y/o impacto.
- El seguimiento y remediación del incidente hasta su resolución.
- La documentación y el análisis de causa raíz del incidente, con la propuesta de acciones de prevención.
- La denuncia del incidente ante las Fuerzas y Cuerpos de Seguridad del Estado (Policía, Guardia Civil) se observe la posible comisión de un delito y/o el incidente sea de elevada peligrosidad y/o impacto o bien cuando se produzca o sea previsible la reclamación por parte de clientes o a la apertura de expediente por Autoridades Reguladoras.

16. Protección de la información

Para evitar la pérdida, robo o transferencia no autorizada de la información clasificada o propiedad intelectual de **SYGRIS**, se seguirán las siguientes medidas:

- La identificación y clasificación de toda la información, en cualquier soporte, considerada de especial protección.
- El seguimiento y supervisión de los controles para el acceso, manejo, transmisión y reproducción de dicha información.
- El seguimiento por los usuarios de una práctica de puesto de trabajo despejado de expedientes y bloqueo de pantalla mediante contraseña cuando el equipo esté desatendido o no esté en uso.

17. Continuidad de las operaciones

Para reducir los riesgos derivados de la ocurrencia de un ciberataque, accidente, catástrofe, atentado o sabotaje se siguen las siguientes medidas:

- La preparación y actualización periódica del plan de continuidad de negocio.
- La difusión y formación sobre las medidas de continuidad de negocio entre el personal y los colaboradores.

18. Cumplimiento legal

Para evitar contingencias legales derivadas del manejo de los datos de carácter personal, se siguen las siguientes medidas:

- La identificación y registro de los requisitos legales o contractuales de aplicación en materia de seguridad de la información.
- El cumplimiento normativo, con especial incidencia, de la legislación vigente en materia de protección de datos personales.
- La auditoría periódica del cumplimiento normativo con el fin de verificar y tener a disposición de reguladores y autoridades las evidencias de cumplimiento.

19. Mejora continua

Para optimizar y mejorar de modo permanente la gestión de la seguridad de la información, se siguen las siguientes medidas:

- Las propuestas de cualquier sugerencia, medida o acción de mejora, por parte de los usuarios son dirigidas al Responsable de Seguridad de la Información.
- El registro y seguimiento, desde su propuesta hasta su cierre, de las mejoras propuestas.
- El análisis periódico de las mejoras propuestas e implantación, en su caso.
- El reconocimiento a los usuarios que propongan mejoras.

20. Actualización, distribución y aceptación

La Política de seguridad será revisada con regularidad anual o, bien, siempre cuando se produzca un cambio significativo, para asegurar su vigencia, idoneidad, adecuación y eficacia.

Los cambios a la Política de Seguridad de la Información serán aprobados por la Dirección de **SYGRIS** y distribuidos puntualmente por el Responsable de Seguridad de la Información.

Para la plena adecuación de las medidas de la presente Política de seguridad de la Información se dispondrá de un plazo de nueve meses a contar a partir de la fecha de su aprobación.
