POLÍTICA DE RESPALDO DE LA INFORMACIÓN

ÍNDICE

1 OBJETIVO

AREA XXI recoge en la presente Política los requisitos para el adecuado y eficaz respaldo de datos e información crítica de negocio en conformidad al control A.12.3.1 de la norma ISO 27001:2013, definiendo las directrices que rigen las acciones de respaldo de datos e información, que permitan la protección de datos y software existentes en los dispositivos de hardware que la soportan, almacenan y distribuyen.

2 ALCANCE

La presente política aplica para la información crítica de negocio declarada o almacenada en los servidores descritos y documentados en el apartado 7.1 siguiente.

3 ROLES Y RESPONSABILIDADES

- **Oficial de Seguridad de la Información (CISO)**
  - Monitorizar, medir y verificar la correcta ejecución de los procedimientos de respaldos.
  - Velar por la ejecución y control de los procesos de respaldo definidos.
  - Coordinar y velar por el correcto desempeño de las pruebas de recuperación programadas.
  - Mantener el inventario de dispositivos, hardware y software, respaldados debidamente actualizados.
  - Velar por la consistencia de los medios de almacenamiento para la solución de respaldo.
- **Comité de Seguridad de la Información (CIS)**
  - Velar por el cumplimiento de la política de respaldo.

4 DEFINICIONES

- **Información**: Conjunto de datos relacionados empleados y/o generados por AREA XXI.

- **Información crítica**: Conjunto de datos relacionados y que proveen o representar valor para el negocio de AREA XXI.
- **Integridad**: Propiedad de la información que busca la protección contra modificaciones no autorizadas a la misma.
- **Disponibilidad**: Propiedad de la información, o el medio que la provee, que referencia al acceso, debidamente autorizado, a la información cuando este sea requerido.
- **Confidencialidad**: Propiedad de la información que impide su divulgación y acceso no autorizado a la misma.
- **Respaldo**: Copia de información a un medio del cual se pueda recuperar y restaurar la información original.
- **Restauración**: Recuperación de parte o la totalidad de información desde una copia de respaldo que permita restaurar un sistema tras un desastre.
- **Inconsistencia**: Hace referencia a que la información que se respalde permita su restauración posterior y no contenga errores lógicos o físicos.
- **Repositorio**: Depósito en un sitio centralizado donde se almacena y mantiene información.
- **Respaldo Full**: Operación de respaldo que almacena una copia integra y completa de toda la información definida.
- **Respaldo Incremental**: Operación de respaldo que almacena una copia integra de todos los cambios o variaciones, realizados a la información, desde la última operación de respaldo realizada sobre la información.
- **Retención**: Periodo de vigencia y/o permanencia de un respaldo de información.
- **Periodicidad**: Frecuencia definida con la que se ejecutarán las operaciones de respaldo.

5 DOCUMENTOS RELACIONADOS

- *SGSI-POL-001, Política General de Seguridad de la Información.*
- *SGSI-PRC-014 Procedimiento de Gestión de Cambios -*

6 CONSIDERACIONES GENERALES

Toda la información que apoya o provee el negocio realizado por AREA XXI debe ser debidamente resguardada de posibles fallos, perdida, robo, alteración y cualquier otra situación que ponga en riesgo la continuidad e integridad de la información generada, producida y empleada por AREA XXI para su contexto de negocio. Lo anterior implica que la información crítica de negocio debe ser debidamente resguardada mediante planes de respaldo programados y definidos los cuales sean auditables, comprobables y medibles y que se encarguen, en todo momento, de mantener y velar por la integridad y confidencialidad de la información respaldada.

Esta labor se realiza por parte de AREA XXI en su aplicativo *AGRA-XXI* y su módulo *GestionRisk*, en los que existen backups definidos, y por parte del proveedor externo, en DROPBOX EMPRESARIAL. También AREA XXI cuenta con un Tenant de Microsoft 365 con licencias E1, Empresa y Básica que proporciona un SharePoint para AREA XXI y un OneDrive para cada licencia de 1 TB de tamaño que se podrá utilizar para futuros balanceos de datos o en sustitución o complemento de Dropbox.

AREA XXI es consciente que existe información empleada y/o generada en estaciones de trabajo laptops de AREA XXI la cual no corresponde con el criterio definido de Información Critica; Esta información no es respaldada al no representar o proveer valor para el negocio.

Está prohibido guardar información relevante para el negocio de AREA XXI fuera de los recursos destinados al efecto, como el DROPBOX EMPRESARIAL de AREA XXI. Referencia: SGSI-POL-001, Política de Seguridad de la Información.

6.1 Respaldos

Los respaldos generados se evidencian mediante las imágenes de los backups en *AGRA-XXI*

y *GestionRisk*, y en la consola de IONOS, en el caso del *TIME*, recibiendo un email en el que se confirma su realización y término correctos.

También se genera una copia diaria de la BBDD de MySQL de AGRA y GESTIONRISK en Producción, dicho respaldo se copia por un script al usuario de DROPBOX habilitado al efecto para mantener la misma en mas de un sistema.

6.2 Registros de Eventos (LOGS)

En los sistemas de información de AREA XXI registrados SGSI-REG-004 Inventario de Activos, que se detallan a continuación se registran los eventos de los sistemas y se pueden generar informes de dichos eventos (LOGS):

- Dropbox Business
- Microsoft 365
- AGRA
- GESTIONRISK
- TIME

Los registros están protegidos contra la adulteración y el acceso no autorizado, solo tiene acceso el administrador de Dropbox y Microsoft 365 así como el administrador de Ubuntu para AGRA, GESTIONRISK y Time, y en los mismos se detalla cuando sea relevante:

a) identificadores (ID) de usuario;

b) actividades del sistema;

c) fechas, tiempos y detalles de eventos clave, por ejemplo, conexión (log-on) y desconexión (log-off);

d) identidad o localización del dispositivo, si es posible e identidad del sistema;

e) registro de intentos de acceso a los sistemas exitosos y fallidos;

f) registro de intentos de acceso a los recursos y a los datos exitosos y fallidos;

g) cambios en la configuración del sistema;

h) uso de privilegios;

i) uso de utilidades y aplicaciones del sistema;

j) ficheros a los que se ha accedido y el tipo de acceso;

k) direcciones y protocolos de red;

l) alarmas generadas por el sistema de control de acceso;

m) activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y de

detección de intrusión;

n) registro de transacciones ejecutadas por usuarios en las aplicaciones.

6.3 Identificación de Información Crítica

La Alta Dirección y los distintos responsables, en coordinación con el oficial de seguridad de la información CISO, determinarán la información que provee valor para el negocio la cual debe ser tratada como Información Crítica, definida en el Apdo.4 anterior, como "*Conjunto de datos relacionados y que proveen o representar valor para el negocio de AREA XXI.*"

Así mismo, el Apdo. 4.2 del SGSI-PRC-002 Clasificación y tratamiento de la información recoge las siguientes categorías de información:

- PÚBLICA: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de AREA XXI o no.
- USO INTERNO: Información que puede ser conocida y utilizada por todos los

empleados de AREA XXI y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para AREA XXI, o terceros.

- CONFIDENCIAL: Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas para AREA XXI, o para terceros.

6.4 Plan de Respaldo

AREA XXI define el respaldo completo de los servidores virtuales que proveen los servicios, aplicaciones y datos para la normal operación del negocio. En este contexto se considera:

- Respaldo de servidores en Cloud: AGRA, GESTIONRISK, TIME.
- Periodicidad: 1 FULL SEMANAL / INCREMENTAL.

Como se ha indicado en el Apdo.6 anterior, los respaldos de servidores de terceros son realizados por el propio proveedor externo, como en el caso de DROPBOX EMPRESARIAL.

- Respaldo Correo Electrónico – Servicio Exchange Microsoft365.
  Servicio de Redundancia de Microsoft -

6.5 Pruebas de Recuperación

AREA XXI define una programación y calendarización para la realización de pruebas de recuperación de la información respaldada con el objetivo de verificar su consistencia e integridad y en el contexto de apoyar la recuperación frente a desastres, continuidad de negocio y disposiciones legales aplicables conforme sea requerido. Para lo anterior se ha definido:

- *SGCN-PRC-001 Plan de Continuidad de Negocio.*
- *SGSI-REG-002 Programa del SGSI y SGCN.*

6.6 Retención

AREA XXI declara que no necesita dar cumplimiento normativo o legal referente al tiempo de retención para los respaldos realizados.

6.7 Caducidad

AREA XXI declara que toda información respaldada, posterior a 5 años de retención, en caso de que exista, puede ser eliminada.

7 ACTIVOS DE INFORMACIÓN

La infraestructura de los servidores de AREA XXI es la siguiente:

Servidor	Ubicación	Servicios	Retención	Responsable
AGRA	IONOS	SERVER	1-2-3 Meses	CISO – M. MEZA
AGRA-LAB	IONOS	SERVER	1-2-3 Meses	CISO – M. MEZA
GESTIONRISK	IONOS	SERVER	1-2-3 Meses	CISO – M. MEZA
GESTIONRISK LAB	IONOS	SERVER	1-2-3 Meses	CISO – M. MEZA
TIME	IONOS	SERVER	1-2-3 Meses	CISO
MICROSOFT 365	MICROSOFT	MAIL	1-2-3 Meses	CISO
DROPBOX	DROPBOX/LOCAL	SERVER	180 Días	CISO

Tabla 1 - Activos de Información

Toda la transferencia de información con Clientes o Partners deberá realizarse por uno de los métodos descritos en la tabla 1, en ningún caso se podrán utilizar como medio de transferencia de información los chats, whatsapp o cualquier otro sistema de mensajería o intercambio no autorizado explícitamente por el CISO previa consulta o petición y su posterior aprobación.

8 SANCIONES

El incumplimiento de la presente política conlleva a un proceso de sanción disciplinaria conforme señala el SGSI-PRC-013 Procedimiento de Sanciones Disciplinarias, documento debidamente comunicado, socializado y aceptado.

9 COMUNICACIÓN E INFORMACIÓN

La presente Política será comunicada a todo el equipo de AREA-XXI, y terceras partes relevantes, en su caso, siendo así mismo publicada en la intranet, o en el repositorio digital de la compañía para facilitar su acceso, dentro del marco general y de los programas de formación y concienciación, en relación al SGSI (Sistema de Gestión de Seguridad de la Información).

Así mismo, cualquier hecho relevante que afecte al cumplimiento de alguna de las obligaciones contempladas en la misma, deberá ser informado de forma expresa a los implicados, así como a los responsables de las distintas Áreas y a la Alta Dirección, quedando constancia por escrito de dichas comunicaciones.

10 REVISIÓN DE LA POLÍTICA

La presente Política será revisada por el Responsable de Seguridad de la Información (CISO), como encargado de la coordinación operativa del SGSI, con el fin de asegurar que se mantiene su idoneidad, adecuación y eficacia, o en caso de que se produzca algún cambio significativo en lo que concierne a este sistema, y como mínimo una vez al año.

Si en algún momento se produce una modificación, será incorporada a este documento, y aprobada por la ALTA DIRECCIÓN, quedando reflejados los cambios en el cuadro del histórico de versiones siguiente.

11 HISTÓRICO DE VERSIONES

Versión	Fecha	Descripción del Cambio	Responsable del cambio	Responsable de aprobación	Fecha de aprobación
00	26/08/2021	Creación del documento	Implementación	No aplica	26/08/2021
01	08/09/2021	Revisión del documento	CISO	CSI	08/09/2021
02	17/03/2020	Revisión del documento	CISO	CSI	18/03/2022
03	01/04/2022	Revisión del Punto 7: Transferencia de información con Clientes o Partners a través de medios seguros.	CISO	CSI	20/04/2022