Procedimiento de desarrollo, mantenimiento y adquisición de sistemas informáticos

CONTROL DE DOCUMENTO	
Copia Controlada	**Revisión Nº**
01	01

APROBACIONES		
Elaborado por:	**Revisado Por:**	**Aprobado por:**
Nombre: Angie Cruz	Nombre: Raul Quevedo	Nombre: Jenny Freire
Cargo: Process and Quality Controller	Cargo: Chief Operating Officer	Cargo: Quality Manager
Firma:	Firma:	Firma:
Fecha:	Fecha:	Fecha:

1. OBJETIVO

Definir las medidas de seguridad y controles para la inclusión de inspecciones de seguridad en el proceso de construcción, mantención, adquisición y explotación de sistemas informáticos.

2. CAMPO DE APLICACIÓN

Están dentro del alcance de esta política, todas las construcciones o adquisiciones de sistemas informáticos por parte de Cercal; así como también, los procesos y servicios de interoperación electrónica, entre Cercal y proveedores y entre las sedes de Cercal.

3. RESPONSABILIDADES

3.1. Definir y dictarlas políticas, estándares en tecnologías, seguridad de la información (integridad y confidencialidad) y su soporte tecnológico, velando por el cumplimiento de las políticas de la seguridad de la información.
3.2. Está a cargo de la seguridad de los sistemas informáticos de Cercal.
3.3. El departamento de informática, en conjunto con los propietarios de la información, son los responsables de definir el nivel de criticidad de los sistemas informáticos, y de identificar los controles de seguridad a aplicar para resguardarlos.
3.4. Revisar, aprobar o rechazar procesos y controles que mitiguen, eliminen o transfieran los riesgos relacionados con la construcción, mantención y adquisición de sistemas informáticos y, según corresponda, definir procedimientos para ello.
3.5. Verificar el cumplimiento de los procedimientos y controles de seguridad establecidos para la construcción, mantenimiento, y adquisición de sistemas informáticos.
3.6. El departamento de informática es el responsable de implementar, mantener, difundir y disponer los mecanismos de seguridad nativos, propios de las plataformas e infraestructura, con el fin de que estos sean utilizados por las aplicaciones que serán desarrolladas para operar sobre estas plataformas.
3.7. El departamento de informática tiene la responsabilidad de definir las normas, procedimientos y controles que permitan asegurar que en los procesos de construcción y mantenimiento de sistemas informáticos se apliquen los controles necesarios para la seguridad de la información de estos, tales como:

- Metodología de análisis.
- Construcción de pruebas unitarias y de integración.
- Administración de sistemas.
- Administración de bases de datos.
- Documentación.
- Sistema de gestión de código.

3.8. El departamento de informática, la gerencia general y las jefaturas de departamento son responsables de promover y verificar el cumplimiento de las políticas de seguridad que se señalan en este documento.
3.9. El departamento de informática en conjunto con la gerencia general, son responsables de especificar, verificar y validar los requerimientos de seguridad que deben cumplir los paquetes de software ofertados en el mercado, independiente de cómo se realiza su adquisición.

4. PROCESO DE DESARROLLO/MANTENIMIENTO DE SISTEMAS INFORMÁTICOS

4.1. El proceso de desarrollo y/o mantenimiento de sistemas informáticos, debe contar con normas de programación como: versión, documentación y pruebas para cada etapa del ciclo de vida (construcción, pruebas, explotación).
4.2. El ciclo de vida del desarrollo y/o mantenimiento de sistemas informáticos debe incluir procedimientos de pruebas funcionales y no funcionales. Las pruebas no funcionales deben incluir las pruebas de seguridad.
4.3. El proceso de desarrollo y/o mantenimiento de sistemas informáticos, así como los procesos de pruebas, deben efectuarse en ambientes dispuestos para ello.
4.4. Los sistemas que interoperen o intercambien datos, con otros sistemas o base de datos, pertenecientes a Cercal o a un tercero, deben contar con controles de seguridad en ambos extremos de la comunicación.
4.5. La responsabilidad del proceso de desarrollo y/o mantenimiento de sistemas informáticos, en particular la programación (codificación), debe tener siempre dos o más responsables de forma que no se detenga el proceso en periodos de vacaciones, licencias médicas o permisos laborales. Es decir, no debe depender de una sola persona.
4.6. El proceso de desarrollo y/o mantenimiento de sistemas informáticos realizados por terceros deben cumplir con esta política y con la política de seguridad de la información, especificada en la sección 12 “Desarrollo y mantenimiento de sistemas”.

5. DOCUMENTACIÓN DE LOS SISTEMAS INFORMÁTICOS

5.1. La documentación de los sistemas informáticos debe obedecer a los lineamientos de documentación definida por las normativas implementadas en de Cercal. Excepciones a esta política, son la adquisición de software empaquetado.
5.2. Toda la documentación asociada al ciclo de desarrollo y/o mantenimiento de sistemas informáticos debe tener procedimientos de control de versión.
5.3. El acceso a la documentación de sistemas de información, bibliotecas de códigos fuente y programas ejecutables, debe estar restringida sólo a personal autorizado. La excepción a esta

política, son los manuales de usuario, manuales de capacitación, u otros documentos destinados a los usuarios del o los sistemas informáticos.

6. ESPECIFICACIONES DE REQUERIMIENTOS DE SEGURIDAD

6.1. Para la construcción de nuevos sistemas informáticos o mejoras a los existentes, se debe especificar los controles de seguridad desde la etapa de levantamiento de requerimientos, tales como encriptación de claves, de mensajes, de configuración, auditoria de trazabilidad, entre otros.
6.2. En la identificación de controles de seguridad deben participar las áreas de la empresa que serán usuarios del sistema informático en construcción o proceso de mantenimiento.
6.3. El diseño e implementación de controles de seguridad deben ser preferentemente de tipo automático, evitando procesos o intervención manuales. Las excepciones deben ser aprobadas por la gerencia general.
6.4. En la etapa de diseño, debe considerarse los procedimientos necesarios para realizar revisiones periódicas de contenidos de campos, registros, tablas o archivos considerados sensibles, frecuencia de los respaldos y tiempos de retención de estos, y procesos de depuración (limpieza de datos, indexaciones, u otros procesos relacionados con optimización y rendimiento).
6.5. Se puede emplear datos de prueba extraídos desde las bases de datos de los sistemas informáticos de Cercal, pero sólo deben ser empleados dentro de las instalaciones de la empresa. Excepciones a esta política, deben ser autorizadas por el dueño de la información, o en su defecto la gerencia general y se deberá elaborar y formalizar un Convenio de confidencialidad por parte de terceros.
6.6. El acceso a las bases de datos de construcción, prueba y producción, deben contar con controles de acceso (autenticación y autorización). Deben definirse quiénes (roles) tienen acceso a las bases de datos en sus diferentes ambientes y qué tipo de acceso (consulta, actualización, eliminación). Jamás en la etapa de construcción y/o prueba se debe dar acceso a los datos de producción.

7. VALIDACIÓN DE DATOS DE ENTRADA Y SALIDA

7.1. En términos generales, todo sistema que considere transformación de datos de entrada debe ser diseñada y construida considerando controles de integridad de éstos.
7.2. Los sistemas que se construyan en Cercal por proveedores, y aquellos sistemas adquiridos, deben contemplar funcionalidades que permita acceder tanto a los registros de auditoría como a los registros de trazabilidad.

7.3. Cuando un sistema tenga previsto el envío de datos (interoperabilidad) que contengan información clasificada como reservada, se debe implementar mecanismos de cifrado de los datos.

8. FIRMA DIGITAL Y DE ENCRIPTACIÓN

8.1. Toda firma digital debe de incluir jeroglífico, nombre completo y fecha en la que se firma.
8.2. El personal de Cercal deberá de estructurar sus firmas digitales bajo el siguiente estándar:

- Jeroglífico en color azul. RGB (46,117,182).
- La letra para el nombre y la fecha debe ser Quincy CF, tamaño 12 y color negro.
- El formato de fecha debe de ser (dd/mm/aaaa).
- El jeroglífico debes de ser una imagen png sin fondo.

8.3. Cualquier contrato y/o acuerdo de confidencialidad debe de incluir en cada una de las páginas la firma digital.
8.4. La firma digital en cada página debe de agregarse sin sobreponerse al texto.
8.5. La fecha de la firma digital debe de ser la misma que la fecha en la que se firma.
8.6. Todo documento firmado digitalmente, debe de ser almacenado por el área de calidad, validando que la última fecha de modificación es coherente con la fecha de firma.
8.7. Se recomienda utilizar la firma digital para documentos que no debieran cambiar con el tiempo.
8.8. Todo documento modificado deberá de ser firmado nuevamente.

9. ADMINISTRACIÓN DE CLAVES

9.1. La administración de cuentas y contraseñas de acceso a los sistemas de información debe ser centralizada. Excepciones a esta política deben ser justificadas por los propietarios de la información, y autorizadas por la gerencia general.
9.2. El mecanismo de autenticación de usuarios de Cercal debe estar basado en una estructura de árboles jerárquicos. Excepciones a esta política deben estar autorizadas por la gerencia general.
9.3. La generación de códigos de cuentas y contraseñas de acceso de los usuarios a los sistemas de información, deben asegurar, a lo menos:
9.3.1. Que los códigos de cuentas sean únicos.
9.3.2.Que la generación de contraseñas cumpla al menos con atributos tales como: largo mínimo, sean alfanuméricas, no repetibles, renovables periódicamente, y que se fuerce su cambio por el involucrado (usuario) cuando se use por primera vez.

9.4. La generación de códigos de cuentas y contraseñas de acceso de los usuarios a los sistemas de información, deben asegurar, a lo menos:
9.4.1. Que los códigos de cuentas sean únicos.
9.4.2.Que la generación de contraseñas cumpla al menos con atributos tales como: largo mínimo, sean alfanuméricas, no repetibles, renovables periódicamente, y que se fuerce su cambio por el involucrado (usuario) cuando se use por primera vez.
9.5. El mecanismo o procedimiento de creación de grupos de usuarios, perfiles o privilegios, entre otros aspectos, deben preferentemente ser administrados en cada sistema de información. Excepciones a esta política deben ser autorizadas por la gerencia general de Cercal.
9.6. La solicitud de códigos de cuentas de acceso a los sistemas de información debe efectuarse según se establece en la sección 11 "control de accesos" de las políticas de la seguridad de la información.

10. CONTROL DE VERSIONES

10.1. Toda la documentación, archivos ejecutables, códigos fuente y bibliotecas de software de los sistemas construidos, script de bases de datos, así como la documentación de paquetes de software adquiridos, debe estar bajo procedimientos de control de cambios y de versión.

10.2. El departamento de informática debe mantener un registro actualizado de todos los sistemas en uso, con datos respecto de versión, fecha de última compilación, responsable(s) de su mantenimiento y soporte.

11. CAMBIOS EN LA PLATAFORMA OPERATIVA

Previo a cualquier cambio, actualización, o reconfiguración planificada en los servidores de aplicaciones, de bases de datos, u otros equipos asociados a la operación de sistemas de información, el departamento de informática debe efectuar un análisis y emitir un informe técnico que evalué los impactos y riesgos que puedan generar estos cambios.

12. ADQUISICIÓN DE PAQUETES DE SOFTWARE

12.1. En el proceso de análisis y adquisición de paquetes de software a terceros, deben considerarse aspectos y atributos de seguridad de la información, y el impacto en la seguridad frente eventuales cambios o modificaciones para su implementación en Cercal.

12.2. Las modificaciones a los paquetes de software o sistemas adquiridos de terceros, que surjan producto de su uso y tengan relación con las políticas de seguridad de la información, tal

como lo especifica la sección 10 "Gestión de operaciones en aplicaciones y cambios", deben ser aprobados la gerencia general.

12.3. Se prohíbe el uso y/o copia de cualquier paquete de software, por parte de los colaboradores de Cercal, del cual no se disponga de su respectiva licencia que lo autorice.

12.4. La instalación de paquetes de software que son denominados "de código abierto" deben ser autorizados por la gerencia general y validados por el departamento de informática con el objeto de determinar si están dentro de los lineamentos de herramientas de software utilizados por Cercal.

13. CAPACITACIÓN

La puesta en producción de los Sistemas informáticos, sean éstos construidos internamente o adquiridos de terceros, deben siempre considerar la realización de actividades de capacitación dirigida a usuarios finales, administradores de plataforma y de la mesa de ayuda.

14. CONTROL DE CAMBIOS

Control De Cambios		
Fecha	**Revisión**	**Descripción del Cambio**
23-12-2019	Rev. 00	- Creación del Documento
07/07/2021	Rev. 01	- Eliminación del subtítulo "3.1. Departamento de informática" - Inclusión de los numerales específicos de las políticas de la seguridad de información que se hace referencia en el punto 5, 10 y 13. - Modificación total de la sección 9 "Firma digital y de encriptación". - Adición de flujo de proceso.