Crédito Regional
Compañía Financiera S.A.

POLITICA DE SEGURIDAD DE LA INFORMACION

Crédito Regional
Compañía Financiera S.A.

Contenido

1. Objetivos de la Política

Esta política tiene como principal objetivo definir un marco que permita proteger los , las Redes y la Información contenida en ellos, accesible en o a través de ellos, de todo tipo de amenazas, ya sean internas, externas, deliberada o accdientalmente.

Los objetivos de la Política se Seguridad de la Información son los siguientes:

- ✓ Toda aplicación crítica para el negocio debe estar alojada en en un entorno seguro y establecer las estrategias necesarias para continuar procesando la información, aún en períodos de indisponibilidad prolongada.
- ✓ Toda información almacenada o intercambiada en los Sistemas debe ser gestionada en forma segura, cumpliendo con los requisitos legales, del ente de contralor y las buenas practicas profesionales
- ✓ Todos los Sistemas y la información asociada a estos, debe estar debidamente protegida contra accesos no autorizados.
- ✓ Todo usuario que utilice los Sistemas y/o Activos Informaticos y de Información debe respetar y cumplir las Políticas de Seguridad de la Información estipuladas por Crédito Regional Compañía Financiera S.A., como así también ser consciente de su responsabilidad en términos de Seguridad de la Información
- ✓ Todos los acuerdos con terceras partes sobre: accesos, almacenamiento, procesamiento, comunicación o gestión de la Información de propiedad de la Entidad o instalaciones de procesamiento de Información deberán cubrir todos los aspectos relevantes sobre seguridad.

Para el cumplimiento de los objetivos anteriormente mencionados se aplicarán los tres pilares básicos de Seguridad de la Información:

- ➢ Confidencialidad
- ➢ Integridad
- ➢ Disponibilidad

2. Alcance de la Política

Esta Política establece los principios de un buen Gobierno de Seguridad. Cualquier documento existente (política, metodología, estándar, acuerdo, etc.) ya implementada, se mantiene en vigencia siempre y cuando no sea contraria a los principios que contiene la presente Política. Son considerados parte integrante de la politica todos aquellos procedimientos que se traten a lo largo de la misma. En consecuencia, esta Política es aplicable a:

- ✓ Todas las áreas o gerencias de la Entidad.
- ✓ Todos los empleados, proveedores, empleados tercerizados, empleados temporarios, etc.
- ✓ Toda la información y datos de las instalaciones de procesamiento de Información (Ej: Todos los Sistemas y Redes utilizados por Crédito Regional Compañía Financiera S.A.).

3. Exenciones a la Política

En circunstancias operacionales excepcionales puede no ser posible cumplir en su totalidad con algunos requerimientos incluidos en la presente Política. Cuando se considere que se puede estar ante esa situación, se deberá efectuar un pedido formal de exención a la Política de Seguridad de la Información.

4. Responsabilidades

Los usuarios tienen responsabilidades explícitas ante la Seguridad de la Información y pueden ser considerados personalmente responsables de sus actos y omisiones en el cumplimiento de esas responsabilidades. Es también Parte de los cargos gerenciales monitorear la conformidad con los requerimientos de la Política de Seguridad de la Información de la Entidad.

5. Gobierno de la Seguridad de la Información

La Gerecia General, a través de su gerencia de Protección de Activos de Información, será quien tenga a cargo el desarrollo e implementación de la Seguridad de la Información.

Principios de Gobierno

El Gobierno de Seguridad de la Información funciona como un nexo estrecho entre el Consejo de Administración y los responsables por la Seguridad de la Información. El Gobierno lleva las iniciativas de Seguridad a través de las gerencias, basándose en los siguientes principios:

- **Alineamiento estratégico** de la seguridad de la información con la estrategia Negocio para dar soporte a las necesidades y objetivos.

- **Gestión del Riesgo** a través de la ejecución de medidas apropiadas para gestionar y mitigar los riesgos y llevar los posibles impactos sobre los recursos de información de la Entidad hacia un nivel de riesgo aceptable.

- **Administración de los Recursos** utilizando los conocimientos sobre seguridad de la Información e infraestructura de manera eficaz y eficiente.

- **Evaluación de la performance** midiendo, monitoreando y reportando a través de métricas de Gobierno de Seguridad de la Información que sean robustas y auditables, para garantizar que los objetivos fueron cumplidos.

- **Entrega de Valor** optimizando las Inversiones de Seguridad de la Información en soporte a los Objetivos de la Entidad y del Negocio.

Teniendo en cuenta los principios anteriormente mencionados, serán responsabilidad del área de Protección de Activos de Información:

- ✓ La definición y actualización de la Estrategia de Seguridad de la Información, la cual deberá estar alineada a las necesidades del Negocio, y los requerimientos de los órganos de contralor.
- ✓ Identificar posibles amenazas que pudieran afectar a los Sistemas y poner de algún modo, la información en riesgo. Asimismo, efectuar y mantener actualizado un análisis de riesgos para determinar el nivel de exposición a los mismos.
- ✓ Implementar un programa de concientización para difundir las reglas en materia de Seguridad de la Información a todas aquellas personas que tengan acceso a los Sistemas de Información.
- ✓ Facilitar la realización de auditorías de Seguridad y cuando fuera necesario, efectuar una revisión de los planes de acción en materia de seguridad de la Información a fin de remediar debilidades o incumplimientos detectados
- ✓ Efectuar reportes en forma periódica que permitan ver un status de los puntos principales en materia de Seguridad de la Información.
- ✓ Reportar y dar seguimiento a los Incidentes de Seguridad que sean considerados como importantes y relevantes.
- ✓ Implementar estándares y desarrollar normas que mejoren la Seguridad de la Información.
- ✓ Establecer los controles de acceso apropiados cada uno de los aplicativos de acuerdo al rol que cada usuario ocupe dentro de la Entidad.
- ✓ Adoptar las medidas que fueran necesarias para mantener en forma segura todos aquellos lugares físicos donde exista equipamiento que contenga Información que sea propiedad de la Entidad.
- ✓ Asistir en el armado de acuerdos de confidencialidad de datos.
- ✓ Asistir en la adquisiscion e implementacion de nuevos recursos tecnologicos, asegurando que los mismos cumplan las condiciones de seguridad necesarias.
- ✓ Establecer estandares para el empleo de utilitarios que permitan el alta, baja o modifiacion de datos operativos, por fuera de los sistemas aplicativos que los orginan.
- ✓ Desarrollar procedimientos que faciliten la prevención, detección y elminación de software malicioso.
- ✓ Establecer medidas de seguridad que permitan detectar intrusos en las redes y plataformas informáticas, así como tambien establecer acciones que deban implementarse luego de su detección.

6. Gestión de Riesgo

Se deberá instrumentar un proceso de gestión del riesgo de seguridad de la información concordante con el contexto, los requerimientos del ente de contralor y los definidos por la Entidad y en particular por el Área de Gestión de Riesgo, que se encuadra con los lineamientos establecidos en el Código de Gobierno Societario, aprobado oportunamente por el Consejo de Administración de la Entidad. El proceso contará al menos con las siguientes etapas:

- Evaluación, seguimiento y revisión del riesgo, a través de un enfoque iterativo proporcionando un equilibrio entre minimizar el tiempo y el esfuerzo en identificar controles, mientras que se asegura que los altos riesgos están evaluados apropiadamente. Se implementará un criterio de valoración del riesgo para evaluar el riesgo de seguridad de la información de la Entidad considerando lo siguiente:

    - El valor estratégico del proceso de la información del negocio
    - La criticidad de los activos de información implicados
    - Requisitos legales y reglamentarios, y obligaciones contractuales
    - La importancia operacional y del negocio de la disponibilidad, de la confidencialidad y de la integridad
    - Las expectativas y las percepciones de las partes interesadas, y las consecuencias negativas para el buen nombre y la reputación

  Como criterio de valoración se implementará una estimación cualitativa, es decir una escala de clasificación de atributos para describir la magnitud de consecuencias potenciales (Baja, Media, Alta) y la probabilidad de que esa consecuencia pueda ocurrir, utilizando la misma escala. Una ventaja de la estimación cualitativa es su facilidad de comprensión por todo el personal relevante.

- Tratamiento del riesgo, proporcionar información suficiente para determinar con eficacia las acciones requeridas para modificar los riesgos a un nivel aceptable. Es posible que el tratamiento del riesgo no conduzca inmediatamente a un nivel de riesgo residual aceptable. En esta situación, de ser necesario, se establecerá un tratamiento del riesgo complementario. Estableciendo para:

    - Riesgos Residuales Bajos, se debe mantener el tratamiento que se realiza hasta el momento de su valuación.
    - Riesgos Residuales Medios, se procedera a mejorar la eficacia o eficienca de los controles actuales con la finalidad de aumentar la percepción de control y disminuir el riesgo residual.
    - Riesgos Residuales Altos, se establecerá un plan de adecuación.

- Aceptación del riesgo. El Consejo de Administración deberá aceptar explicitamente la totalidad de los riesgos residuales, especialemente donde se omite o pospone implementar controles ya sea por temas estrategicos, presupuestarios o relacionados costo/beneficio del control.

- Comunicación del riesgo. Es importante que los riesgos y su tratamiento sean comunicados al personal de la Entidad. La concientización acerca de los riesgos, la naturaleza de los controles implementados para mitigarlos ayuda en el tratamiento de incidentes y eventos inesperados en forma más efectiva.

7. Reglas de Seguridad de la Información

Las reglas sobre Seguridad de la Información detalladas en la presente Política cumplen con el estándar definido en los Requisitos Mínimos de Gestión, Implementación y Control de los Riesgos Relacionados con Tecnología Informática, Sistemas de Información y Recursos Asociados para las Entidades Financieras establecidos por el Banco Central de la República Argentia y Norma ISO 27002. De todas maneras, la relevancia e importancia de cada regla está determinada de acuerdo al riesgo específico de la Entidad y su implementación se encuentra sujeta a revisiones periódicas.

La gestión sobre Seguridad de la Información de Crédito Regional Compañía Financiera S.A. se basa en el siguiente principio:

Las acciones tomadas en materia de Seguridad de la Información están orientadas a proteger las actividades del negocio y su información, en forma proporcional al riesgo en el cual se incurra contemplando los requerimientos mínimos establecidos por el órgano de contralor

En consecuencia, Crédito Regional Compañía Financiera S.A. invierte en controles a la Seguridad de la Información en aquellos casos donde realmente sea justificado. El objetivo no es eliminar por completo los riesgos de Seguridad, sino minimizar los posibles impactos a través de un proceso efectivo y rentable. Un riesgo de Seguridad puede estar caracterizado por un accidente, un error o un acto malintencionado que pudiera poner en peligro:

- ✓ La **Confidencialidad**, previniendo la divulgación de la información a individuos o Sistemas no autorizados a recibirla.

- ✓ La **Integridad**, cuidando la exactitud, integridad y actualidad de los activos de Sistemas (Software e Información).

- ✓ La **Disponibilidad**, asegurando que la información y los servicios esenciales se encuentran accesibles a los usuarios autorizados cuando así lo fuera requerido.

- ✓ La **Trazabilidad**, asegurando que las acciones o procesos realizadas por los usuarios sobre la información relevante, son registradas bajo el nombre de cada uno de estos, a fin de que las consecuencias de las mismas puedan ser vinculadas a los usuarios en cuestión y de esta manera, los mismos, ser responsable por sus acciones.

8. Responsabilidad de los Usuarios de la Información

Tal como fuera mencionado en el apartado “Alcance de la Política de Seguridad”, la misma es aplicable a empleados, externos bajo cualquiera de sus formas (tercerizados, contratados, consultores, contratistas, etc.) y terceros. Todos ellos, son responsables del tratamiento lícito de la información que gestionan (producen, manipulan y/o distribuyen), siendo responsables en todo momento por la confidencialidad y la integridad de la misma. Todos ellos están en conocimiento de las reglas de Seguridad de la Información que deben ser aplicadas.

También deberán cumplir con todas las normas y políticas en materia de seguridad de la Información establecidas por la Entidad, siendo responsables de la protección de sus usuarios y contraseñas de los Sistemas de Información frente a acciones que pudieran ser malintencionadas y utilizando la información únicamente para los fines autorizados.
Es también responsabilidad de los usuarios reportar cualquier actividad que consideren sea de carácter sospechosa o cualquier incidente de Seguridad que pudiera ser detectado.

Los usuarios recibirán la formación adecuada para poder dar cumplimiento a sus responsabilidades.

9. Seguridad en Contratos

En todos aquellos contratos donde esté involucrado el tratamiento de Información (almacenamiento, transferencia y/o procesamiento) que sea propiedad de Crédito Regional Compañía Financiera S.A., se deberá cumplir con los requisitos de Seguridad establecidos a tal fin.

Para ello, existen cláusulas de Seguridad de la Información en poder de la Gerencia de Protección de Activos de Información que deberán ser anexadas en cada contrato que involucre tratamiento de la información de la Entidad en cualquier formato (impreso o digital).

a. Tercerización en la Gestión de la Información

Será de vital importancia mantener la seguridad de la Información cuando la responsabilidad sobre el tratamiento de la misma quede en manos de terceros. Para ello deberán existir acuerdos de confidencialidad y contratos con cláusulas que contemplen riesgos, controles a efectuar y procedimientos de Seguridad, cada vez que se opte por este tipo de Servicios.

Los proveedores que sean seleccionados para este tipo de operaciones deberán garantizar que están en condiciones de cumplir con los requisitos establecidos y que darán conformidad a las cláusulas impuestas por Crédito Regional Compañía Financiera S.A. antes de ser contratados efectivamente.

b. Requisitos mínimos

Los requisitos de Seguridad ante cualquier tipo de Servicio subcontratado que involucrare gestión de la Información propiedad de la Entidad, deberán ser volcados de manera explícita en el carácter vinculante de los contratos que se efectuaren. Los mismos deberán incluir cláusulas para:

- ✓ Asegurar la continuidad del servicio
- ✓ Mantener un adecuado nivel de servicio
- ✓ Dar conformidad a la confidencialidad de la Información
- ✓ La trazabilidad de punta a punta y la protección de los Sistemas de Información interconectados.

10. Protección de la Información

Toda la Información almacenada o procesada que sea propiedad de Crédito Regional Compañía Financiera S.A. debe ser debidamente protegida, cualquiera sea el entorno donde ella se encuentre.

a. Necesidades de Seguridad

La Información almacenada o procesada por las aplicaciones críticas del negocio y por cualquier tipo de Servicio, debe ser clasificada de acuerdo a su criticidad para el negocio. Para ello, deberá ser identificada y clasificada de acuerdo a su confidencialidad, integridad, disponibilidad y trazabilidad.

b. Impacto en el Negocio

El impacto en el negocio de divulgación no autorizada de información y la corrupción accidental o manipulación deliberada de la información almacenada o precesada por las aplicaciones, debe ser auditada.

c. Propiedad

La propiedad de la Información crítica debe ser asignada a individuos capaces con responsabilidades claramente definidas y aceptadas, para obtener de ellos el compromiso en la protección de la Información crítica de la Entidad. Deberán aplicarse controles de Seguridad que mantengan el riesgo en un nivel aceptable.

d. Privacidad

Toda información que sea catalogada como de carácter personal deberá ser manipulada conforme a lo dispuesto por la Ley Nacional de Protección de datos Personales N° 25.326 y posteriores Leyes o Decretos de ampliación y/o modificación. Se debera establecer la responsabilidad en la gestión de la privacidad de la Información y deberán aplicarse los debidos controles en el manejo de la Información que sea catalogada como “personal”.

e. Almacenamiento

La información guardada en medios de almacenamiento (incluyendo cintas magneticas, discos, informes impresos, etc.), deberá ser protegida contra corrupción, pérdida o divulgación. Se deberán establecer controles de Seguridad apropiados para proteger los medios que contengan información crítica.
Se deberá controlar e impedir la salida de equipamiento, datos y software que no estuvieran previamente autorizados por un responsable.

f. Cifrado de Datos

Se deberá utilizar criptorgrafía para:

- Proteger la confidencialidad de la Información Crítica
- Determinar si la información crítica ha sido alterada
- Proveer autenticación fuerte para usuarios de aplicativos y Sistemas
- Permitir que la identidad de quien genera información crítica sea demostrada

11. Seguridad en Soportes de Información

Un punto esencial en la protección de activos de información, es establecer procedimientos que protejan los soportes de Información, datos de entrada y salida, documentación interna de carácter sensible y confidencial, contra posibles daños, robos y accesos no autorizados, con el fin de proteger la información y evitar interrupciones en la actividad de la Entidad. Para ello, es vital contar con medidas de Seguridad en:

- Gestión de soportes de información removibles, entendiendo como soporte u otro medio removible y transportable a: discos duros externos, laptops, agendas electrónicas, copias de respaldo, memorias externas o informes en soporte papel. Se debe guardar un registro de los mismos y se deben almacenar en forma segura con las medidas de seguridad que corresponda aplicar en cada caso, cuando la información se encontrare en soporte físico y en tránsito fuera de las instalaciones de la Entidad, como por ejemplo, las copias de respaldo ubicadas en un lugar físico alejado del centro de procesamiento de datos principal, tal lo establecen las buenas prácticas en Seguridad de la Información.
- Los soportes que contengan copias de respaldo, deberán estar correctamente etiquetados, indicando la fecha en la que se realizó el Back Up, la información que contiene y el/las áreas que son propietarias de dicha información.
- El borrado Seguro de soportes, cuando se pueda prescindir de ellos, mediante procedimientos de borrado seguro de información (desmagnetización de cintas, eliminación de datos de discos duros, compactación, destrucción, incineración, etc.), ya sea realizado por personal de la Entidad o por terceros especializados en este tipo de tareas, los cuales deberán ser supervisados por personal de la Gerencia Protección de Activos de Información.
- Seguridad en la documentación de los sistemas de proceso de datos para proteger la información sensible (Aplicaciones, estructuras de datos, tec) mediante un almacenamiento y un control de acceso de usuarios autorizados.

12. Concientización a usuarios

Los usuarios deberán estar formados y concientizados sobre los elementos clave en lo que respecta a la Seguridad de la Información y el por qué es necesario estar alerta. De esta forma serán capaces de entender su responsabilidad personal frente a la seguridad de la Información para asegurar que los controles de seguridad más relevantes son aplicados y para poder prevenir que la información crítica sea comprometida o divulgada a individuos no autorizados.
Para ello se utilizarán todos los canales de comunicación posibles y poder llegar de manera clara con los mensajes a los usuarios. Se deberá efectuar un plan anual de capacitación al personal orientado según las necesidades de cada gerencia que forman parte de la Entidad.

c. Reglas de Seguridad

Los colaboradores deberán ser provistos de una guía que los ayude a comprender e incorporar en su accionar cotidiano los conceptos de:

- El Significado de la Seguridad de la Información, haciendo especial hincapié en lo que respecte a la protección de la información y la confidencialidad de la misma, su integridad y su disponibilidad.
- La importancia de cumplir con la Política de Seguridad de la Información y la aplicación de sus estándares asociados junto con los procedimientos y normas existentes.
- Su responsabilidad personal frente a la seguridad de la Información, recalcando la importancia de reportar cualquier incidente relacionado con la seguridad de la información.

d. Ética

Los usuarios de los aplicativos deberán estar concientizados sobre la prohibición que existe en:

- El uso no autorizado sobre la Información y los Sistemas
- La utilización de las aplicaciones para propósitos que no sean los estrictamente laborales.
- Realizar declaraciones que fueran de carácter sexual, racista, discriminatorias, obscenas, de acoso u otro tipo de declaraciones que pudieran ser ofensivas para la moral y las buenas costumbres, por ejemplo, cuando se utiliza el correo electronico, la mensajería instantánea, Internet, o Telefonía de Voz.
- La utilización no autorizada de servicios o equipamiento, como pudiera ser la utilización de software de terceros, memorias de tipo USB, modems o cualquier equipamiento o software no autorizado o licenciado por Crédito Regional Compañía Financiera S.A.

- La realización de copias no autorizadas sobre información o software que sea propiedad de Crédito Regional Compañía Financiera S.A.
- La divulgación de información confidencial que sea propiedad del Crédito Regional Compañía Financiera S.A. como pueden ser Datos de Clientes, diseños de productos, formulas, precios, promociones, etc., a individuos o terceros no autorizados.
- Comprometer cualquier tipo de password que haya sido otorgada por la Entidad para el desempeño de las funciones de cada uno de los colaboradores, por ejemplo, dejandolas a la vista de cualquier otra persona o compartiéndola.
- Manipular evidencia que pueda ser de vital importancia en la investigación forense de un incidente de seguridad.

e. Programa de Concientización sobre Seguridad de la Información

Desarrollar y mantener un programa de concientización en materia de Seguridad de la Información para todos aquellos individuos que tienen acceso a la Información y los Sistemas, y que sea inclusivo a todos los niveles jerárquicos de la Entidad, prefesionales de Sistemas y personal externo en cualquiera de sus formas (tercerizados, contratados, personal de Servicios, etc).

13. Gestión de Identidad y Accesos

Un mecanismo efectivo en el control de accesos a la información reduce considerablemente el riesgo de accesos no autorizados a los Sistemas y a la Información. En consecuencia, este apartado cubre las medidas aplicadas sobre los usuarios en materia de control de accesos y los pasos que deben seguirse para poder restringir el acceso a la Información según un modelo basado en Roles.

a. Aprovisionamiento de Cuentas a Usuarios

Se deberán establecer controles sobre la gestión de identidades y accesos a los aplicativos para gestionar de forma consistente y efectiva la administración de usuarios de los aplicativos de Crédito Regional Compañía Financiera S.A.
El aprovisionamiento proporciona a los usuarios con las cuentas y derechos de acceso que los mismos necesitan para el normal desempeño de sus funciones.

El procedimiento de gestión de identidades deberá ser capaz de que los dueños de los aplicativos puedan gestionar los privilegios de accesos a los usuarios de los mismos. A tal efecto deberá establecerse un método para que los superiores sean capaces de otorgar o revocar dichos accesos.

Los usuarios deberán notificar cualquier incidente relacionado con la seguridad en la contraseña, ya sea pérdida, robo o indicio de falla de la confidencialidad.

b. Ingreso a los Sistemas

Deberá existir un proceso de logueo a los aplicativos antes de que los usuarios sean provistos del acceso a los mismos, el cual deberá referir a un único ID por cada individuo.

c. Autenticación de usuarios

Se deberá definir un estandar de autenticación que será utilizada en los procesos de logueo que deberá ser avalada por los estándares establecidos por el Banco Central de República Argentina.
Los usuarios administradores y los usuarios de aplicaciones críticas deberán poseer, siempre y cuando sea posible, un doble factor de autenticación.
Deberá existir un proceso de recupero y cambio de password que asegure que la divulgación de la password es mínima cuando ésta sea comunicada a los usuarios finales. El usuario debe cambiar su contraseña ante cualquier indicio de trascendencia de la misma, o solicitar el cambio de su contraseña al área de seguridad informática si no pudiera realizarlo por sí mismo.
La información sobre ID’s y Passwords no deberá ser asignada en forma colectiva, excepto que alguna circunstancia especiale así lo requiera.

d. Principios de Acceso

Todos los derechos de acceso deberán ser autorizados por un superior siempre que sea técnicamente posible, o por un superior con cargo de Gerente. La presente política prohibe todo tipo de acceso que no haya sido autorizado por un superior.

Los usuarios de Aplicativos deberán ser provistos con los accesos mínimos e indispensables para la realización de sus funciones.

e. Control de los Accesos

El acceso a las aplicaciones críticas del Crédito Regional Compañía Financiera S.A., servicios e información, deberá estar restringido unicamente a los individuos autorizados. Los derechos de acceso de los usuarios deberán ser:

- ✓ Restringidos a su rol en la Entidad
- ✓ Autorizados por el dueño del proceso o el aplicativo
- ✓ Revocados en forma inmediata cuando los mismos se desvinculan de la Entidad o cuando cambian de funcion dentro de la misma. A tal efecto, los dueño del proceso o el aplicativo serán responsables por comunicar tales situaciones.
- ✓ Efectuar revisiones períodicas con el objeto de:
  - Cancelar identificadores y cuentas de usuarios redundantes
  - Inhabilitar y/o eliminar cuentas inactivas

En caso de existir excepciones deberán ser debidamente justificadas y aproabadas.
En ningún caso los privilegios deben ser otorgados hasta que se haya completado el proceso formal de autorización.

14. Seguridad en el Equipamiento de Sistemas

Los niveles de Servicio objetivo que brinda todo el equipamiento de Sistemas son mas factibles de ser alcanzados siempre y cuando toda la Infraestructura esté bien diseñada.

a. Gestión y Clasificación de Activos

Dentro de la clasificación y valorización de activos de Información, se deberá establecer la criticidad de los mismos efectuando dos valorizaciones:

- ✓ Valorización estratégica del proceso de cara al Negocio
- ✓ Valorización efectuada sobre los tres pilares de Seguridad de la Información

    - **Confidencialidad:** Refiere al nivel de sensibilidad que posee la Información
    - **Integridad:** Refiere a un posible impacto por cambios no autorizados en la Información, corrupción de los datos, etc., basándose en el principio de que la Información solo puede ser modificada por los sujetos autorizados a tal fin.
    - **Disponibilidad:** Refiere a que la Información debe estar disponible cuando el Negocio así lo requiera.

Todo Hardware y Software que pertenezca a la Entidad deberá formar parte de un inventario actualizado.

b. Configuración del Equipamiento de Sistemas

Todo el equipamiento de Sistemas de Información deberá ser configurado en términos de Seguridad, para su funcionamiento tal cual lo requerido por las buenas prácticas y por las políticas que así lo establecen. Esto evitará que se realicen actualizaciones no autorizadas o incorrectas y permitirá que todo el equipamiento opere tal cual lo esperado sin poner en riesgo la seguridad de los mismos, de la información que contienen o de la Entidad.

c. Gestión de Parches de Seguridad

Se deberá establecer un proceso para la instalación de parches de seguridad de Sistemas Operativos y de Aplicativos para subsanar cualquier tipo de vulnerabilidad que pudiera existir en forma rápida y eficaz, para reducir con esto la probabilidad de ocurrencia de cualquier impacto serio que pudiera ocurrir sobre las actividades del negocio. El proceso de gestión de parches hará posible la distribución en forma masiva de los mismos sin importar la plataforma de la cual se trate, cupliendo con los requisitos de tiempo y forma para este proceso.

Cuando se producen cambios en los Sistemas Operativos, las aplicaciones críticas de negocio deben ser revisadas y testeadas para asegurar que no existe un impacto adverso en las operaciones o la seguridad. La implementación de los cambios en los servidores de producción se realiza en forma manual, previa prueba en servidores determinados para tal fin. En las estaciones de trabajo, la actualización se realiza en forma automática.

d. Soluciones de urgencia a vulnerabilidades

Cualquier solucion de emergencia a cualquier vulnerabilidad que pueda existir en sistemas operativos, bases de datos, aplicativos o cualquier otro tipo de software o información del negocio, y que deba aplicarse, deberá ser revisada, testeada y aplicada en forma rápida y efectiva de acuerdo a los estándares o procedimientos que existan documentados para tal fin. Es importante en este proceso llevar a un nivel mínimo el impacto sobre el negocio.

e. Protección anti Malware

Se deberá contar con un software antimalware para prevenir la propagación de código malicioso y evitar impactos al negocio. Este software deberá ser instalado, configurado y mantenido en aquellos Sistemas que sean susceptibles de ser atacados.

f. Gestión de LOGS o Pistas de Auditoría

Los eventos que sean caracterizados como importantes en relación a la Seguridad, deberán ser guardados en pistas de auditoría o LOGS, protegidos contra un cambio no autorizado y analizados de manera regular para identificar posibles amenazas que pudieran derivar en un incidente de Seguridad.
Los eventos de Seguridad deberán ser guardados en pistas de auditoría cuando se tratare de:

- ✓ Sistemas que son críticos para la Entidad, como por ejemplo bases de datos con información financiera o disposiitivos clave de comunicaciones,
- ✓ Sistemas que hayan experimentado algún tipo de incidente de Seguridad de consideración,
- ✓ Sistemas que son objeto de asuntos legales o de algún tipo de regualción o que se encontraren con información que sea de vital importancia y prueba en algun tipo de litigio en el cual la Entidad o alguno de sus colaboradores estuvieran involucrados.

g. Protección física del equipamiento

Todo el equipamiento que alojare Sistemas o Aplicaciones que sean consideradas críticas para el negocio, información sensible y/o confidencial o cualquier otro tipo de material que fuera considerado como tal, deberá estar físicamente protegido cumpliendo con los requerimientos de seguridad física y ambiental. Los acuerdos firmados con terceros para el hosting de Equipamiento y/o aplicativos, deberán incluir en alguna de sus cláusulas los requisitos que deben ser cumplidos por el prestador de los servicios para estos casos (sistemas de refrigeración, sistemas anti incendio, sistemas de energía redundante, etc.), en caso respetando las especificaciones de sus proveedores.

La protección física se llevará a cabo mediante la creación de diversas barrera o medidas de control. El perimetro estará delimitado por una barrera y existirá una puerta de acceso controlado por dispositivos de autenticación o antendido por personas.

- ✓ solo podrá acceder personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
- ✓ Se deben revisar y actualizar los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable del Área restringida.
- ✓ Se deberá evitar la ejecución de trabajos por parte de terceros sin supervisión.
- ✓ Está Prohibido comer, beber y fumar dentro de las instalaciones de procesamiento de la información. Se deberá ingresar con equipamiento adecuado para combatir incendios en las áreas protegidas.
- ✓ Se implementarán los mecanismos necesarios para proteger el acceso al cableado troncal (backbone) así como a los racks de comunicaciones mediante cajas con cerraduras.
- ✓ Los empleados tendrán acceso a sus áreas de trabajo exceptuando las zonas declaradas críticas.

h. Adquisicion de nuevos recursos informaticos

Frente a la adquisicion de nuevos recusos informaticos el area de Proteccion de Activos de Informacion es responsable sobre las medidas de seguridad que se apliquen sobre el mismo, asi como de verificar y asegurar que todo recurso a incorporar cumpla los estanders de seguridad establecidos por la Entidad, proveedores y entes reguladores.

i. Ambientes de Producción

Los ambientes de producción deberán estar separados de los ambientes de desarrollo y de testing.

j. Operación de los Sistemas

El logro de los niveles de servicio requiere de plataformas de sistemas que se ejecuten de acuerdo con lo esperado. Los siguientes procedimientos deben establecerse y mantenerse en forma actualizada:

- ✓ gestión del cambio,
- ✓ mantenimiento de hardware y software,
- ✓ gestión de incidentes,
- ✓ gestión de copias de seguridad y
- ✓ gestión segura eliminación de datos y dispositivos declarados inservibles.

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- ✓ Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor.
- ✓ Mantener un listado actualizado del equipamiento con el detalle y frecuencia en que se realizará el mantenimiento preventivo a fin de que no se vea afectada la operatoria normal de la Entidad.
- ✓ Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
  Será necesario evaluar, antes de realizar cualquier tarea de mantenimiento, recaudos complementarios por las carracterísticas de la información alojada o el procesos de negocios al que brinda soporte ese equipamiento.
- ✓ Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado. - Registrar el retiro de equipamiento de la sede de la Entidad para su mantenimiento.
- ✓ Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

15. Plan de Continuidad del Negocio

En caso de que existiera una interrupción en el procesamiento de la información de la Entidad los sistemas podrían estar indisponibles por un largo período de tiempo. Para ello será necesario estar preparados para poder habilitar el procesamiento de datos en el menor tiempo posible y con el menor impacto posible al negocio. Este apartado enumera los puntos que deberán ser tenidos en cuenta a la hora de desarrollar un plan de contingencia.

a. Resiliencia

Es importante que las Aplicaciones que resultan críticas para el negocio deben ser ejecutadas sobre entornos que sean robustos y confiables (Hardware y Software) y soportados por servicios redundantes.

b. Back Up - Copias de Respaldo

Las copias de respaldo de la información que resulta esencial para el desarrollo del negocio, como así tambien del software utilizado por las aplicaciones críticas. Estas copias deberán estar alojadas en lugares seguros destinados a tal fin (ignifugos, libres de humedad, de acceso restringido, etc.), y deberán testearse regularmente para garantizar que los datos son recuperables cuando fuere necesario hacerlo.

c. Contingencia

Deberá existir en la Entidad un plan de recuperación ante desastres para todas las aplicaciones críticas del negocio, o servicios de Sistemas de Información, para aquellos casos en los cuales se tratare de una emergencia.

d. Continuidad del Negocio

Para que la Entidad pueda seguir con sus operaciones ante una indisponibilidad prolongada en sus sistemas de Información y su información crítica, deberá existir un plan de continuidad de Negocio que contemple una operación manual o restringida. Este plan deberá ser actualizado con la periodicidad de al menos un año.

e. Gestión de Crisis

Deberá existir un procedimiento para la gestión de crisis en la Entidad, el cual deberá estar operacional para poder gestionar los incidentes mayores en los Sistemas de Información.

f. Testing

Lo planes de continuidad de negocio y de recuperación ante desastres (BCP y DRP), deberán ser probados y testeados regularmente, con una periodicidad de al menos un año, despues de cada actualización. Los Testeos deberán incluir simulaciones reales con participáción de usuarios del negocio y personal de Sistemas, para poder demostrar que el procesamiento de la información puede reanudarse en un tiempo razonable.

16. Seguridad en las Aplicaciones del Negocio

Las aplicaciones que resultan críticas para el negocio requieren de un análisis profundo en materia de seguridad de la información, mucho más riguroso que cualquiera del resto de las aplicaciones. A través de un entendimiento de los impactos probables al negocio, en materia de pérdida de confidencialidad, integridad o disponibilidad de la información, es posible poder establecer un nivel de importancia para cada uno de los aplicativos de la Entidad. De esta manera se podrán identificar los riesgos de la información y poder así determinar cual es el nivel de protección que se debe adoptar para mantener esos riesgos en su nivel mínimo aceptable.

a. Requerimientos de desarrollo por parte del Negocio

Los requerimientos del negocio deberán tener en cuenta las políticas, normas, estándares y procedimientos actuales en materia de Seguridad de la Información. Los dueños de las aplicaciones del negocio, los responsables por la seguridad de la información, los líderes de proyecto y el personal que será responsable por el mantenimiento del aplicativo, deben dar su consentimiento explícito para cualquier desarrollo que sea requerido sobre estos.

b. Análsis de Riesgos

Las aplicaciones que resultaren críticas para el negocio, como así también el equipamiento de Sistemas que resulta de carácter crítico, las redes y demás aplicaciones y procesos que transaccionen con información crítica, deberán ser objeto de un análisis de riesgo en forma regular, que permita al propietario del aplicativo y al propietario de la información identificar los principales riesgos y determinar los controles que fueren necesarios para mantener los riesgos dentro de una de límite aceptable.

c. Seguridad en los proyectos

La metodología de desarrollo e implementación de sistemas o modificaciones a los mismos, deberán incluir las definiciones en materia de seguridad de la información que resultaren pertinentes durante la etapa de definición o de requerimientos, diseño y construcción de los mismos, como así también la etapa de pruebas y las actividades relacionadas a la implementación de los mismos.

d. Transferencia de Datos

La transferencia de información sensible, que involucre aplicaciones críticas o con terceros deberán contemplar la utilización de criptografía para:

- ✓ Proteger la confidencialidad de la información cuando la misma sea transferida
- ✓ Determinar si la información ha sido alterada durante su traspaso a terceros o entre aplicativos
- ✓ Garantizar la no manipulación de datos que se transfieran entre aplicativos.

e. Aplicaciones basadas en Web

Se deberán aplicar procedimientos y controles de seguridad especialmente diseñados para este tipo de aplicativos y servidores donde son ejecutados para minimizar los riesgos asociados a este tipo de aplicativos, dado que su exposición es mayor a aquellos aplicativos que solo son operados dentro de la red de Crédito Regional Compañía Financiera S.A.

f. Pistas de Auditoria (Logs) de Aplicativos

Las actividades críticas de los usuarios de aplicativos deberán quedar registradas en pistas de auditoría. Los eventos deberán ser configurados para:

- ✓ Grabar los tipos de eventos que sean apropiados, como pueden ser: fallo inesperado y abrupto de los sistemas, borrado de objetos, intentos de logueo fallidos, intentos de acceso no autorizados, etc.
- ✓ Incorporar atributos relevantes para los eventos que vayan a ser objeto de grabado como pistas de auditoría (Ej: Direcciones IP, identidad del usuario, fecha y hora, protocolo y puertos utilizados, archivos o utilidades del Sistema accedidas, utilizadas, modificadas, método de conexión, nombre del dispositivo y nombre del objeto, etc.)

17. Seguridad en Redes de Comunicación

Las Redes de telecomunicaciones transmiten la información de la Entidad y proporcionan un canal de acceso a los Sistemas de Información. Por su propia naturaleza e interconectividad son declaradas de alta vulnerabilidad ante interrupciones e intrusiones. Para proteger la información del negocio y el desarrollo de las comunicaciones dentro de éste, las Redes deben ser armadas y configuradas de manera robusta, los servicios bien definidos, su tráfico identificado, comportamientos que deben ser observados y deberá tener una excelente gestión de la seguridad de la red.

a. Resiliencia

Las redes deben ser ejecutadas y estar soportadas por equipamiento (hardware y software) que sea robusto y confiable, poseer servicios alternativos o duplicados para un caso de contingencia y garantizar de esta manera que la red se encuentra disponible en los casos que el negocio así lo requiera.

b. Segregación de la Red

El Tráfico que se genere en la red deberá estar ruteado a través de un firewall configurado con las reglas que hayan sido previamente establecidas en función de las necesidades de tráfico de la Entidad, y antes que ingrese o salga de la red.

c. Exploradores de Internet

Aquellas estaciones de trabajo que se conecten a Internet deberían estar protegidas por exploradores de Internet que posean una configuración de Seguridad aplicada por política corporativa y que no permita cambios en los niveles de seguridad por parte de un usuario final. Se deberán incorporar a la política de gestión de parches de seguridad aquellas actualizaciones o correcciones a vulnerabilidades de seguridad sobre los Exploradores de Internet.

d. Correo Electrónico

Los sistemas de correo electrónico deberán ser protegidos por políticas de concientización, procedimientos y medidas de seguridad tecnica junto con controles que garanticen que el servicio de correo se encuentra disponible cuando es necesario. Otro aspecto importante a cubrir será la confidencialidad y la integridad de los mensajes en tránsito, como así también garantizar que el riesgo por una utilización indebida en este servicio es reducido a la mínima expresión como ser:

- Enviar cadenas de mensajes
- Enviar mensajes de seguridad que no fueron originados por la Gerencia de Protección de Activos de Información.

- Relacionarse con actividades ilegales y no éticas de acuerdo al uso, la moral y las buenas costumbres
- Enviar mensajes no relacionados con los propósitos de la Entidad

e. Detección de Intrusos

Se deberán activar mecanismos para la detección de intrusiones en la red. Estos mecanismos deberán ser utilizados para la protección de redes y aplicaciones críticas y poder así identificar tipos de ataques que sean predeterminados, como así también nuevas modalidades de ataque.

f. Trabajo Remoto

Todo el equipamiento utilizado por el personal de Crédito Regional Compañía Financiera S.A. para el acceso remoto deberá estar homologado, es decir que sean confiables y protegido por controles físicos y lógicos que aseguren que estos dispositivos operan tal cual lo esperado y no pongan en compromiso ninguno de los servicios a los cuales se están conectando en los entornos de Crédito Regional Compañía Financiera S.A.

g. Accesos de Terceros (Third party)

Las conexiones que se mantengan con terceros (Ej: proveedores de servicios, redes LAN to LAN con proveedores, etc.) deberán ser individualmente identificadas y sujetas a evaluación de análisis de riesgos. Los términos del acceso a los terceros deberán quedar registrados en el contrato de carácter formal que da sustento legal a la operación en cuestión.

h. Acceso a Redes inalámbricas (Wireless)

Los usuarios deberán autenticarse al ingresar en la red, y el tráfico deberá estar encriptado utilizando un método de encripción fuerte y de esta forma asegurar que solo los usuarios identificados acceden a la red, minimizando el riesgo de que las transimisiones de datos en las redes inalámbricas sean interceptadas y/o modificadas.

18. Gestión de Incidentes

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a esta Política.

Al presentarse un fallo o incidente es obligación, de acuerdo a lo establecido en el alcance de esta politica, reportar el mismo a la brevedad posible.

El área de Protección de Activos de Información deberá implementar un proceso sistemico con el fin de minimizar la ocurrencia futura de los mismos eventos y facilitar la recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, mejorar continuamente el marco de seguridad y el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

19. Mejora de la Política de Seguridad de la Información

Revisiones y actualizaciones a la política de Seguridad de la Información

La presente política deberá ser revisada anualmente y re aprobada, teniendo en cuenta aquellas circunstancias que hayan cambiado en algún aspecto y deban ser incluidos en la presente política. Estas pueden ser:

- ✓ Cambios significativos en el entorno del negocio o en la estrategia.
- ✓ Cambios significativos en el entorno de la seguridad de la Información
- ✓ Cambios en las leyes o regulaciones que afectaren al procesamiento de la información, en el gobierno de Sistemas, etc.
- ✓ Incidentes importantes de Seguridad que hayan impactado en la Entidad.

Todas las revisiones que se realicen y cualquier tipo de cambio sobre la presente política deberá ser validado y aprobado por el Comité de Sistemas y el Consejo e Administración de la Entidad.