Normas Específicas de Seguridad de la Información y Ciberseguridad

ÍNDICE

PROPÓSITO

Establecer un conjunto de normas específicas en el ámbito de Seguridad de la Información, a partir de la **"Política para la Gestión Integral del Riesgo Operacional y Tecnológico".**

ALCANCE

Esta norma es aplicable a todas las unidades que se conecten a la red del banco y/o consulten, procesen o almacenen sus activos de información críticos.

DOCUMENTOS DE REFERENCIA

- ✓ Política para la Gestión Integral del Riesgo Operacional y Tecnológico.
- ✓ Estándares de Seguridad de la Información.

NE01. ORGANIZACIÓN DE LA SEGURIDAD

PROPÓSITO

Establecer roles y responsabilidades para la adecuada gestión de la Seguridad de la Información y Ciberseguridad.

DOCUMENTOS DE REFERENCIA

Política para la Gestión Integral del Riesgo Operacional y Tecnológico.

NORMAS

1.1 Organización Interna

1.1.1 Definición de roles y responsabilidades

BEC24H mantiene definidas todas las responsabilidades de seguridad de la información, conforme a lo indicado en el Capítulo de Roles y Responsabilidades de la "Política para la Gestión Integral del Riesgo Operacional y Tecnológico".

Responsable del Activo de información: Debe de mantener la confidencialidad, integridad y disponibilidad de los activos de información críticos que se encuentran bajo su gestión. Corresponde a un Gerente o Subgerente de BEC24H.

1.1.2 Segregación de funciones

El nivel de acceso asignado a los usuarios debe cumplir con el propósito del negocio y ser consistente con la "Política para la Gestión Integral del Riesgo Operacional y Tecnológico" y las "Normas Específicas de Seguridad de la información y Ciberseguridad".

1.1.3 Contacto con autoridades y grupos de interés

BEC24H debe mantener un adecuado nivel de contacto con las fuerzas de Ley, entidades reguladoras y proveedores de servicios, con el fin de promover el intercambio de información, así como también con agrupaciones y entidades especialistas relacionadas a la Seguridad de la Información y Ciberseguridad, de tal manera de asegurar la actualización en esta materia.

1.1.4 Seguridad de la Información en administración de proyectos

BEC24H debe incorporar dentro de la administración de proyectos aspectos de seguridad de la información para aquellos proyectos que involucren acceso, manipulación o almacenamiento de información confidencial.

1.2 Dispositivos y Trabajo móviles

1.2.1 Dispositivos móviles

Bajo ninguna circunstancia está permitido la conexión de medios o dispositivos móviles, ya sean de propiedad de BEC24H, de funcionarios o pertenecientes a terceras partes, a la red de BEC24H sin previa autorización de la Subgerencia/Gerencia respectiva.

1.2.2 Trabajo Móvil

BEC24H debe implementar medidas de seguridad para proteger la información a la que se accede, procesa o almacena en modalidad de trabajo móvil.

El personal de BEC24H que cuente con equipamiento móvil debe tomar medidas de seguridad.

NE02. SEGURIDAD EN LOS RECURSOS HUMANOS

PROPÓSITO

Definir los lineamientos de seguridad y ciberseguridad antes, durante y luego de finalizada la relación laboral de los empleados con BEC24H.

DOCUMENTOS DE REFERENCIA

- ✓ Política para la Gestión Integral del Riesgo Operacional y Tecnológico.
- ✓ Guía para Efectuar Investigaciones.
- ✓ Reglamento Interno de Orden, Higiene y Seguridad.

NORMAS

2.1 Antes del empleo

2.1.1 Selección

El proceso de selección de personal debe considerar aspectos legales, normativos y éticos considerando además los riesgos asociados a la información a la cual accederá el nuevo empleado y los requisitos del negocio.

2.1.2 Términos y condiciones de empleo

Los contratos entre BEC24H, sus empleados y terceras partes, deben considerar aspectos relacionados con la seguridad de la información y ciberseguridad en la declaración de responsabilidades por ambas partes.

2.2 Durante el empleo

2.2.1 Responsabilidades de la dirección

BEC24H debe velar porque sus empleados y terceras partes cumplan con los lineamientos indicados en los ámbitos de Seguridad de la Información y Ciberseguridad de la "Política para la Gestión Integral del Riesgo Operacional y Tecnológico" y en este documento de normas específicas.

2.2.2 Concientización y capacitación sobre la seguridad de la información y ciberseguridad

BEC24H debe entregar regularmente a sus empleados recursos de capacitación que permitan reforzar sus conocimientos en el ámbito de la seguridad de la información y ciberseguridad, así como el cumplimiento de la "Política para la Gestión Integral del Riesgo Operacional y Tecnológico".

2.2.3 Proceso disciplinario

BEC24H debe establecer dentro de su política de recursos humanos un proceso disciplinario formal a aplicar en caso de incumplimiento de la "Política para la Gestión Integral del Riesgo Operacional y Tecnológico". El cual se encuentra descrito en el "Reglamento Interno de Orden, Higiene y Seguridad" y se encuentra sustentado por la "Guía para Efectuar Investigaciones".

2.2.4 Responsabilidades del personal

El personal de BEC24H debe cumplir con los lineamientos indicados en los ámbitos de Seguridad de la Información y Ciberseguridad de la "Política para la Gestión Integral del Riesgo Operacional y Tecnológico" y del presente documento de normas específicas y sus estándares.

El personal de BEC24H y sus jefaturas deben cumplir con los lineamientos indicados en "Solicitud y Aprobación de Vacaciones o Permisos Administrativos".

Es responsabilidad del usuario cuidar y proteger los equipos tecnológicos de la filial.

Está prohibido:

- ✓ Ingresar sitios web que puedan afectar la seguridad e imagen de la Filial y de la Corporación BancoEstado.
- ✓ Descargar o instalar software no licenciado en los PCs conectados a la red de BancoEstado.
- ✓ Compartir la clave de usuario de acceso a los sistemas provistos por la corporación.
- ✓ Hacer uso o difusión de la información sensible de la filial, BancoEstado y sus clientes en redes sociales.
- ✓ Almacenar en las estaciones de trabajo cualquier archivo (música, videos, imágenes, etc.) que esté sujeto a derecho de autor o propiedad intelectual.

2.3 Término de relación contractual y cambio de empleo

Los contratos entre BEC24H, sus empleados y terceras partes, deben establecer además las responsabilidades sobre la confidencialidad de la información que debe mantenerse una vez finalizada la relación contractual entre ambas partes, o cuando haya un cambio en dicha relación.

NE03. CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN

PROPÓSITO

Establecer los lineamientos para la adecuada administración de activos de información de acuerdo con su importancia para el negocio, a través de la definición de los niveles de clasificación de la información.

ALCANCE

Esta norma es aplicable a todos los activos de información de BEC24H de:

- ✓ Usuarios Internos.
- ✓ Usuarios Externos, en el caso que el dueño de la información apruebe el acceso.
- ✓ Procesos, aplicaciones y/o servicios.

DOCUMENTOS DE REFERENCIA

Estándares de Seguridad de la Información.

NORMAS

3.1 Responsabilidad sobre los activos

3.1.1 Inventario de activos

BEC24H debe mantener un inventario con todos los "activos de información" críticos para el negocio y actualizarlo de forma periódica de acuerdo con el documento "Estándares de Seguridad de la Información", apartado "Estándar de Clasificación de Activos de Información".

3.1.2 Propiedad de los activos

Los distintos "activos de información" deben tener asignado un responsable, que debe velar por su integridad, disponibilidad y confidencialidad.

El "Responsable de Proceso" debe mantener clasificada la información desde el punto de vista de su integridad, confidencialidad y disponibilidad, con el fin de gestionar su protección de acuerdo a su clasificación definida en el documento "Estándares de Seguridad de la Información", apartado "Estándar de Clasificación de Activos de Información".

3.1.3 Uso aceptable de los activos de información

Los usuarios deben hacer uso de los activos de información de acuerdo con lo estipulado en el documento "Estándares de Seguridad de la Información", apartado" "Estándar de Clasificación de Activos de Información".

3.1.4 Devolución de activos

Todos los empleados y usuarios externos deben devolver todos los activos de información de BEC24H que se encuentren en su poder al finalizar su empleo, contrato o acuerdo.

3.2 Clasificación de la información

3.2.1 Niveles de clasificación de la información

Integridad: En lo que respecta al atributo de integridad, los activos de información de la filial deben ser íntegros.

Disponibilidad: BEC24H clasifica su información en 3 niveles:

- ✓ **Nivel 1:** Activos de información que son imprescindibles para la operación de la filial y para las cuales se requiere continuidad.
- ✓ **Nivel 2:** Activos de información que son importantes para BEC24H, pero que pueden mantener una discontinuidad por un período limitado de tiempo.
- ✓ **Nivel 3:** Activos de información que no son críticos para la operación de BEC24H y para las cuales no se requiere continuidad.

Confidencialidad: BEC24H clasifica su información en las siguientes categorías y subcategorías:

Información Confidencial: Dependiendo del grado de restricción que corresponda aplicar, la información confidencial se subclasifica en las siguientes categorías:

- ✓ **Nivel 1**: Es la información que requiere el mayor nivel de restricción por cuanto su divulgación a terceros permitiría acceder directamente a información que posibilita la realización de operaciones en perjuicio de la filial, el Banco o de sus clientes.
- ✓ **Nivel 2:** Es la información protegida por la Ley General de Bancos, Título XVI, "Secreto Bancario y otras Normas". Su divulgación podría tener repercusiones en la responsabilidad legal del Banco, con todos los efectos colaterales que esta situación pudiera acarrear.
- ✓ **Nivel 3:** Es información protegida por las siguientes leyes:

- Ley N°19.628 sobre protección de datos de carácter personal, Título III.
- Ley N°19.496 sobre protección a los derechos de los consumidores, Título III Párrafo3.
- Ley N°17.336 sobre propiedad intelectual – Artículo 3.

También es información protegida por cláusulas contractuales de confidencialidad o calificada como tal por la filial o el propio Banco, su divulgación puede producir efectos directos en la responsabilidad legal, reputación la filial y del Banco, en el desarrollo de las estrategias comerciales y puede otorgar ventajas indebidas a competidores del Banco o a terceros.

- ✓ **Nivel 4:** Es información referida a la filial o al Banco que es distribuida internamente para el conocimiento de sus funcionarios sin restricciones.

Información Pública: Es aquella de libre disposición fuera de la organización, ya sea porque así lo ha establecido la ley o así lo ha dispuesto el dueño o responsable de dicha información.

3.2.2 Etiquetado de información

Todos los "activos de información" críticos de BEC24H, ya sean físicos o electrónicos, deben contar con una identificación de acuerdo al documento "Estándares de Seguridad de la Información" apartado "Estándar de Clasificación de Activos de Información".

3.2.3 Medidas de protección sobre los activos

BEC24H establece medidas de protección de la Información que le permiten garantizar su integridad, confidencialidad y disponibilidad.

3.3 Manejo de Medios

3.3.1 Manejo de medios extraíbles o Medios de almacenamiento masivo

El uso de dispositivos de almacenamiento masivo se encuentra restringido y debe ser autorizado por el Responsable del proceso.

Los dispositivos de almacenamiento masivo que contengan información de BEC24H deben estar protegidos en todo momento contra el acceso no autorizado, el uso indebido o daño, inclusive durante su transporte.

Todo nuevo funcionario que ingrese a BEC24H debe tener bloqueado el acceso a dispositivos de almacenamiento masivo.

3.3.2 Eliminación de medios

Para la eliminación de activos de información, se debe utilizar las indicaciones en documento "Estándares de Seguridad de la Información" apartado "Estándar de Borrado y Destrucción Segura de Información".

3.3.3 Transferencia de medios físicos

BEC24H debe establecer las medidas de protección para los medios que contienen información confidencial, de tal forma que estén protegidos contra el acceso no autorizado, el uso indebido o la corrupción durante el transporte, de acuerdo a lo establecido en el documento "Estándares de Seguridad de la Información", apartado "Estándar de Clasificación de Activos de Información".

NE04. CONTROL DE ACCESO

PROPÓSITO

Definir los lineamientos de seguridad para evitar el acceso lógico no autorizado a la información digital de BEC24H.

ALCANCE

Esta norma es aplicable a todo el personal interno o terceras partes que tenga acceso a la información de BEC24H a través de equipamiento computacional.

DOCUMENTOS DE REFERENCIA

Estándares de Seguridad de la Información.

NORMAS

4.1 Requisitos para el control de acceso

4.1.1 Lineamientos de control de acceso

La administración de usuarios y permisos debe ejecutarse conforme a procedimientos formalmente establecidos y con niveles de autorización previamente definidos.

La administración de usuarios debe cubrir todo el ciclo de vida de los usuarios, desde el registro inicial de un nuevo usuario hasta su eliminación.

4.1.2 Control de acceso a redes y servicios de red

BEC24H debe contar con controles que protejan la información dispuesta en las redes de información y los servicios interconectados, evitando así accesos no autorizados.

Debe existir un adecuado nivel de segregación funcional que regule las actividades ejecutadas por cualquier relacionado, sean estos usuarios personal de la filial o personal externo de servicios.

Cualquier acción crítica en la Plataforma o infraestructura de seguridad de la filial, debe cumplir con los protocolos de autorización establecidos. Entendiéndose como protocolos de autorización, el visto bueno del Subgerente/Gerente a cargo.

Deben estar establecidas las responsabilidades para el acceso remoto a la red de BEC24H, en conformidad con el documento "Estándares de Seguridad de la Información", apartado "Estándar de Control de Acceso".

Las conexiones remotas deben estar protegidas por métodos de autenticación robustos.

Deben existir mecanismos de seguridad sobre la información de BEC24H que se transfiere por las redes públicas.

Todo tipo de conexión remota a los sistemas internos de BEC24H, debe cumplir con lo indicado en el documento "Estándares de Seguridad de la Información", apartado "Estándar de Control de Acceso".

Deben existir controles que impidan el acceso a redes con contenido ilícito que atenten contra la ética, moral o imagen de la corporación BancoEstado.

4.2 Administración de acceso a los usuarios

4.2.1 Registro y cancelación de registro de usuarios

Todo usuario que acceda a los Sistemas de Información de BEC24H, debe tener asignado un identificador único ("User ID"), que permita establecer responsabilidades individuales en el uso de los sistemas de información.

BEC24H debe disponer de los medios necesarios para que el personal y terceras partes puedan crear o modificar sus claves de acceso en forma segura.

4.2.2 Entrega de acceso a los usuarios

BEC24H para asignar y revocar los accesos a sistemas y servicios que se otorgarán a los trabajadores considerará los siguientes aspectos:

- ✓ La asignación de cargo por parte de la Subgerencia de Recursos Humanos, además de la indicación del servicio al cual se integrará el trabajador, para la solicitud de creación del usuario.
- ✓ La verificación de si el acceso cumple con políticas de acceso definidas.
- ✓ Que garantice que el acceso no es otorgado hasta que finaliza el proceso de autorización.
- ✓ Que mantenga registro de los puestos de trabajo otorgados.
- ✓ Que elimine acceso de los usuarios que han terminado su relación contractual.
- ✓ Que modifique los accesos de los usuarios que cambian de función.
- ✓ Que se revisen en forma periódica los accesos otorgados.

No se permite que los usuarios de la filial tengan permisos de "Administración Local" de su estación de trabajo asignada.

4.2.3 Administración de derechos de acceso privilegiado

En BEC24H, se entiende por **cuentas de altos privilegios** (CAP) todas aquellas cuentas de usuario de altas atribuciones que administran el hardware y software de la infraestructura y plataformas tecnológicas (telecomunicaciones, seguridad, servidores, bases de datos, aplicativos, storage) para el negocio, cuyos permisos permiten cambiar las configuraciones y realizar mantenciones sobre ellas, como crear, consultar, modificar y/o borrar: datos, cuentas, claves, logs de eventos, fechas y horas de sistemas, accesos.

Estas acciones significan un riesgo para la integridad, disponibilidad y confidencialidad de los activos de información, por lo cual deben ser monitoreadas.

Dado lo anterior, se deben cumplir los siguientes requerimientos de seguridad:

BEC24H debe contar con mecanismos de monitoreo a los usuarios que cuentan con privilegios de administrador de sistema o base de datos.

Deben existir controles que aseguren que los profesionales que desempeñan funciones relacionadas con tecnologías de información tengan acceso a la información estrictamente necesaria para la ejecución de las labores específicas del cargo.

Deben existir registros de las actividades ejecutadas por los especialistas informáticos, a fin de realizar monitoreo sobre el adecuado uso de los permisos especiales que éstos poseen producto de la naturaleza de su función.

El monitoreo de las actividades de las cuentas de altos privilegios se debe realizar de acuerdo a "Procedimiento de Gestión Monitoreo de Cuentas con Altos Privilegios".

Se debe mantener un "Log" que registre las actividades de los Administradores de Datos, el cual debe ser protegido, respaldado y monitoreado periódicamente por los responsables designados, de acuerdo a lo indicado en el documento "Estándares de Seguridad de la Información", apartado "Estándar de Log de Eventos".

4.2.4 Administración de los mecanismos de autenticación de los usuarios

Los Sistemas de información de BEC24H deben contar con mecanismos de identificación y autenticación de usuarios, incluyendo a aquellos usuarios conectados desde la red externa.

Los procedimientos y herramientas tecnológicas utilizadas para la custodia de claves de acceso deben asegurar su confidencialidad e integridad.

4.2.5 Revisión de los derechos de acceso de usuarios

Cualquier cambio de posición o función de un rol, amerita una evaluación de los permisos asignados, con el fin de realizar las modificaciones que correspondan en forma oportuna.

4.2.6 Eliminación o ajuste de los derechos de acceso

Deben existir procedimientos de eliminación de usuarios o deshabilitación de sus accesos, ante la finalización de la relación contractual con BEC24H.

Una vez finalizada la relación contractual, las cuentas de usuarios de personal desvinculado deben ser deshabilitadas en el proceso nocturno siguiente a la desvinculación.

Semestralmente se solicitará que sean eliminadas las cuentas de usuarios no vigentes en forma definitiva en el Active Directory. Lo anterior podrá ser excepcionado, con la autorización del Gerente de cada área.

Las cuentas de correo electrónico de personal desvinculado se deben mantener al menos deshabilitadas, a excepción de cuentas de ejecutivos (gerentes y subgerentes), las cuales pueden permanecer activas hasta 60 días para la continuidad del negocio.

Los usuarios que cambien de roles y funciones dentro de BEC24H tienen un máximo de 10 días hábiles para habilitar sus nuevos permisos y eliminar los anteriores.

4.3 Resguardo de información de autenticación

Los usuarios deben resguardar la información de sus claves de acceso según lo indicado en el documento "Estándares de Seguridad de la Información", apartado "Estándar de Control de Acceso".

Los usuarios deben ser responsables de todas las acciones que se hayan efectuado bajo su identificación de usuario ("User ID") de acuerdo al concepto de "no repudio".

4.4 Control de acceso a sistemas y aplicaciones

4.4.1 Restricción de acceso a la información

Todo usuario debe tener un puesto de trabajo asignado acorde al cargo y las funciones que desempeña.

BEC24H debe contar con controles que protejan la información dispuesta en las bases de datos de las aplicaciones, evitando así accesos no autorizados.

Debe existir un adecuado nivel de segregación funcional que regule las actividades ejecutadas por los administradores de datos.

Los usuarios deben acceder a la información contenida en las bases de datos, únicamente a través de aplicaciones que cuenten con mecanismos de control que aseguren el acceso a la información autorizada.

4.4.2 Procedimientos de inicio de sesión seguros

El acceso a los sistemas y aplicaciones de BEC24H debe estar controlado por un procedimiento de inicio de sesión seguro.

Las sesiones de usuario deben contar con mecanismos automáticos de bloqueo frente a un período de inactividad determinado.

Cuando se requiera un nivel alto de autenticación y verificación de identidad, se deben utilizar métodos alternativos a las contraseñas, tales como medios criptográficos, tarjetas inteligentes, tokens, o medios biométricos, etc. Los cuales se encuentran descritos en el documento "Estándares de Seguridad de la Información", apartado "Estándar de Control de Acceso".

4.4.3 Sistema de administración de contraseñas

Las claves deben estar protegidas contra acceso y modificación no autorizada, pérdida y destrucción, de acuerdo con el documento "Estándares de Seguridad de la Información", apartado "Estándar de Control de Acceso".

Está prohibido revelar la clave de usuario a terceros, tal como lo indica el documento "Estándares de Seguridad de la Información" apartado "Estándar de Control de Acceso".

4.4.4 Control de acceso al código de fuente del programa

El acceso al código de fuente de programas, y documentación asociada, se debe controlar con el fin de evitar cambios no autorizados, de acuerdo al documento "Estándares de Seguridad de la Información", apartado "Estándar de Desarrollo Seguro de Software".

NE05. SEGURIDAD FISICA Y AMBIENTAL

PROPÓSITO

Prevenir acceso físico no autorizado, daños a las instalaciones o interrupciones al procesamiento de información.

Prevenir la pérdida, daño o compromiso de activos de información como asimismo evitar interrupciones de las actividades del negocio.

ALCANCE

Esta norma es aplicable a todas las instalaciones y equipos de BEC24H en donde se maneje información relevante desde el punto de vista de sus atributos (confidencialidad, integridad y disponibilidad).

DOCUMENTOS DE REFERENCIA

Estándares de Seguridad de la Información.

NORMAS

5.1 Áreas seguras

5.1.1 Perímetro de seguridad física

Las instalaciones de procesamiento de información que manejen información confidencial deben estar protegidas contra interrupciones o acceso físico no autorizado, a través de la implementación de un perímetro físico de seguridad.

5.1.2 Controles de entrada física

Las áreas de procesamiento de información confidencial deben contar con controles de acceso que aseguren el ingreso sólo de personal autorizado.

5.1.3 Protección de oficinas, salas e instalaciones

Todos los lugares en los que se declare trabajar con información confidencial deben contar con medidas que eviten el acceso del público y personal no autorizado, y de amenazas externas y ambientales.

5.1.4 Trabajo en áreas seguras

BEC24H debe diseñar y aplicar procedimientos para trabajar en áreas seguras.

5.1.5 Áreas de entrega y carga

- Las áreas de recepción y despacho deben ser controladas y en la medida de lo posible, aisladas de áreas que manejen información confidencial, para evitar el acceso no autorizado.

5.2 Equipos

5.2.1 Ubicación y protección de equipos

El equipamiento debe estar ubicado en lugares en donde se reduzca la posibilidad de que éstos sean utilizados por personas sin autorización.

5.2.2 Servicios básicos de apoyo

Los servidores y equipos de comunicaciones deben estar protegidos contra fallas u anomalías eléctricas, que evite la pérdida de información o daño físico.

5.2.3 Seguridad del cableado

El cableado de datos y electricidad asociados al equipamiento e instalaciones, deben estar protegidos ante posibles intercepciones de la información, así como de los posibles daños físicos.

5.2.4 Mantenimiento de equipos

Debe existir un proceso periódico de mantención de los equipos, que cumpla con las especificaciones e intervalos recomendados por el fabricante.

Las mantenciones o reparaciones deben ser efectuadas sólo por el personal autorizado.

Previo a la realización de actividades de mantención preventiva o correctiva de equipos, el usuario debe respaldar y proteger la información contenida en los mismos.

5.2.5 Retiro de activos

Debe existir un proceso para el retiro de equipos, la información o el software, de manera que éste no se retire de un lugar sin una autorización previa.

5.2.6 Seguridad de los equipos y los activos fuera de las oficinas

El retiro de cualquier equipamiento de propiedad de BEC24H fuera de sus instalaciones debe ser autorizado.

5.2.7 Eliminación o reutilización segura de equipos

Todo equipo o dispositivo de almacenamiento dado de baja o reutilizado debe someterse a los procedimientos existentes en el área de Soporte Tecnológico de la filial. A fin de garantizar que se haya eliminado de forma segura la información contenida en ellos.

5.2.8 Política de escritorios y pantallas limpios

Debe existir un mecanismo automático de protección de la sesión de usuario luego de un período de inactividad.

Toda documentación que contenga información confidencial debe ser almacenada en un mobiliario seguro.

Los lineamientos para el borrado y destrucción segura de los medios donde se almacenan datos confidenciales en BEC24H se encuentran detallados en el documento "Estándares de Seguridad de la Información", apartado "Estándar de Borrado y Destrucción Segura de la Información".

NE06. SEGURIDAD DE LAS OPERACIONES

PROPÓSITO

Establecer los lineamientos de seguridad para garantizar el correcto procesamiento de las operaciones.

ALCANCE

Esta norma es aplicable a las instalaciones de procesamiento de información de BEC24H.

DOCUMENTOS DE REFERENCIA

Estándares de Seguridad de la Información

NORMAS

6.1 Procedimientos y responsabilidades operacionales

6.1.1 Procedimientos operativos documentados

Se deben documentar los procedimientos de operaciones considerando como mínimo aspectos de instalación y configuración, almacenamiento, procesamiento y respaldo de información, monitoreo de sistemas y manejo de incidentes. Estos procedimientos deben ser actualizados en forma periódica y estar disponibles para el personal.

Las responsabilidades de operación deben estar adecuadamente segregadas a fin de reducir las posibilidades de mal uso o modificaciones no autorizadas a los procesos o información.

6.1.2 Administración de cambios

Todo cambio en la operación de BEC24H, procesos comerciales, instalaciones de procesamiento de información y/o sistemas que afecten a la seguridad de la información debe ser documentado, y autorizado por la Alta Administración de BEC24H.

6.1.3 Administración de la capacidad

BEC24H debe monitorear permanentemente la capacidad de procesamiento de sus instalaciones, con el fin de evitar interrupciones mayores en el negocio.

Además, se deben proyectar los futuros requerimientos de capacidad de procesamiento, tomando en cuenta nuevos negocios, sistemas y cambios en los actuales procesos.

6.1.4 Separación de entornos de desarrollo, pruebas y operacionales

Los ambientes de desarrollo, test y certificación deben estar separados del ambiente de producción.

El acceso directo a los datos del ambiente de producción debe ser restringido, de acuerdo al documento "Estándares de Seguridad de la Información", apartado "Estándar de Control de Acceso".

6.2 Protección contra malware

Todo dispositivo que se conecte a la red de BEC24H debe contar con software de protección contra malware debidamente actualizado.

6.3 Respaldo de información

Los activos críticos de información deben ser debidamente respaldados, garantizándose su disponibilidad, de acuerdo a los lineamientos establecidos en el documento "Estándares de Seguridad de la Información", apartado "Estándar de Respaldo de Información".

6.4 Registro y monitoreo

6.4.1 Registro de eventos

Los sistemas de BEC24H que manejen, almacenen o procesen información deben poseer logs o registro de eventos, de acuerdo a los lineamientos indicados en el documento "Estándares de Seguridad de la Información apartado "Estándar de Log de Eventos".

6.4.2 Protección del registro de información

La información del registro de eventos debe estar protegida contra la adulteración y el acceso no autorizado, según lo indicado en el documento "Estándares de Seguridad de la Información", apartado "Estándar de Log de Eventos".

6.4.3 Registros del administrador y del operador

Las actividades efectuadas por los operadores o usuarios de sistema deben quedar registradas, con el fin de realizar un monitoreo permanente y contribuir a las investigaciones internas.

6.4.4 Sincronización con relojes

Los relojes de los distintos sistemas informáticos de BEC24H deben estar debidamente sincronizados a fin de garantizar la homogeneidad en el registro de los distintos eventos de estos.

6.5 Instalación y actualización de software

Deben existir procedimientos para controlar la instalación de software con el fin de minimizar el riesgo de corrupción del sistema operativo y del resto de las aplicaciones.

Debe existir un registro detallado de todas las actualizaciones realizadas al sistema operativo y a las aplicaciones.

La actualización del sistema operativo o librerías de programas deben ser realizado sólo por personal autorizado y con autorización de la Subgerencia de Planificación y Control o Gerencia/Subgerencia responsable del sistema o programa.

Está prohibida la instalación de software en los equipos de BEC24H, que no esté autorizado por la Subgerencia de Planificación y Control o Gerencia/Subgerencia responsable del sistema o programa tal como indica el "Estándares de Seguridad de la Información", apartados "Estándar de Seguridad para Estaciones de Trabajo" y "Estándar de Seguridad en Servidores".

Los equipos, estaciones de trabajo y servidores deben contar con un proceso de actualización periódico de parches de seguridad.

6.6 Administración de vulnerabilidades

BEC24H debe realizar de forma periódica procesos técnicos de análisis de vulnerabilidad a los sistemas que almacenen o procesen información de clientes, poniendo especial énfasis a aquellos sistemas que tengan exposición directa a redes públicas, pre y post producción.

6.7 Consideraciones sobre la auditoría de los sistemas de información

Toda actividad de auditoría de sistemas debe ser planificada a fin de minimizar el impacto en la continuidad del negocio.

NE07. SEGURIDAD DE LAS COMUNICACIONES

PROPÓSITO

Garantizar que la información que es transmitida a través de medios de comunicación mantenga sus principios de confidencialidad, integridad y disponibilidad.

ALCANCE

Esta norma es aplicable a toda información que es transmitida entre áreas de BEC24H, Corporación BancoEstado y/o con terceras partes.

DOCUMENTOS DE REFERENCIA

"Estándares de Seguridad de la Información".

NORMAS

7.1 Administración de la seguridad de redes

7.1.1 Controles de red

BEC24H debe administrar y controlar las redes para proteger la información de sus sistemas y aplicaciones propias y/o corporativas.

Deben existir controles que aseguren la disponibilidad de los servicios de red y computadores conectados a ésta red corporativa.

Todo computador o equipo portátil que se conecte a la red de BEC24H, debe contar con una identificación única asignada que permita su individualización.

Todo Proveedor que preste servicios a BEC24H, debe realizar la conectividad, gestión y cumplimiento de seguridad tal como indica el "Estándares de Seguridad de la Información" apartado "Estándar de Sistema de Control de Acceso Perimetral".

BancoEstado Contacto 24 Horas S.A. debe controlar y generar logs automáticos y auditables de los perfiles de usuarios utilizados para acceder y administrar la infraestructura de redes y equipos perimetrales relacionados a seguridad y comunicación disponibles en la red interna. En el caso de la red corporativa los logs son generados y administrados por BancoEstado.

7.1.2 Seguridad de los servicios de redes

Cada vez que se implemente un nuevo servicio de red se deben identificar todos los requisitos y controles de seguridad asociados a la prestación del mismo.

7.1.3 Segregación en las redes

BEC24H debe establecer una segregación de los grupos de servicios de información, usuarios y sistemas de información en las redes, tal como indica el "Estándares de Seguridad de la Información" apartado "Estándar de Desarrollo Seguro de Software".

7.1.4 Disponibilidad de Redes

Las redes con las cuales opera BancoEstado Contacto 24 Horas S.A. son entregadas y administradas por la corporación BancoEstado, quienes deben asegurar la alta disponibilidad de estas, siendo responsabilidad de la Filial reportar problemas en la disponibilidad de las redes.

7.2 Transferencia de información

7.2.1 Requisitos para el intercambio de información

Los acuerdos de intercambio de Información entre áreas de BEC24H, Corporación BancoEstado y/o con terceras partes, deben realizarse conforme a lo estipulado en el "Estándares de Seguridad de la Información" apartado "Estándar de Transferencia de Información", lo cual es aplicable a todas las formas de intercambio de información.

No está permitido intercambiar información a través de la red desde las estaciones de trabajo, utilizando carpetas compartidas en forma local en las estaciones de trabajo, lo anterior sólo podrá ser ejecutado previa autorización por la Jefatura del área y gestionado por el área de Soporte tecnológico de la Filial, y para los servidores de recursos compartidos no está permitido que las carpetas estén compartidas con "acceso total para todos los usuarios".

El uso de carpetas compartidas en servidores se debe realizar conforme a los estipulados en el "Estándares de Seguridad de la Información" apartado "Estándar de Seguridad para Servidores".

No está permitido compartir información a través sitios de internet abiertos (nubes públicas como por ejemplo Googledrive).

7.2.2 Mensajería electrónica

Los sistemas de correo electrónico utilizados en BEC24H deben contar con las consideraciones de seguridad descritas en el "Estándares de Seguridad de la Información" apartado "Estándar de Correo Electrónico".

BEC24H debe contar con mecanismos de seguridad en las transacciones electrónicas que son realizadas a través de sus redes y sistemas.

Sólo se permitirá el acceso al correo electrónico corporativo y a sistemas de BEC24H desde computadores portátiles y dispositivos móviles que hayan sido autorizados previamente por el Responsable del Proceso, y que cumpla con los siguientes criterios:

- ✓ Personas que pasan gran parte de su tiempo laboral fuera de las instalaciones donde desempeña sus funciones.
- ✓ Personas que por motivo de contingencia o soporte tecnológico requieran acceso fuera de horario laboral.

- No es aceptable el uso del correo electrónico para enviar información reñida con la ley o la moral.
- No es aceptable el uso de casillas de correo personales para enviar o recibir información propia de las funciones prestadas en BEC24H.
- No se permite la distribución a través del correo electrónico de cadenas de venta, propaganda política, social, religiosa u otra similar.
- No se permite el envío de mensajes o imágenes con pornografía, comercio sexual u otro similar.
- No se permite el envío de programas que violen los derechos de autor (copyright) o programas no licenciados.
- No se permite la creación de reglas de derivación automática de correo hacia casillas no corporativas.
- No se permite el envío de enlaces, URL o códigos QR mediante correo electrónico o mensajería electrónica tal como SMS u otra desde casillas corporativas y cuentas de mensajería oficiales del Banco. Para compartir información, publicaciones de terceros, estudios que aparecen en la red, y otros, el mecanismo alternativo autorizado consiste en enviar la dirección como texto y no como URL.
- Está prohibido enviar, por cualquier medio, URL, links o códigos QR a clientes en nombre del Banco.
- El personal de BEC24H debe seguir los lineamientos de seguridad de Correo electrónico descritos en el "Estándares de Seguridad de la Información" apartado "Estándar de Correo Electrónico".
- Los usuarios deben ser responsables de todos los mensajes que se hayan enviado bajo su identificación de usuario ("User ID") de acuerdo al concepto de "no repudio".

7.2.3 Acuerdos de confidencialidad

BEC24H debe suscribir acuerdos de confidencialidad en los servicios que se presten con terceras partes.

7.2.4 Uso de internet

El acceso a sitios web que permiten descarga y/o transferencia de archivos desde internet serán restringido (Gmail, Facebook, twitter, etc.), a fin de evitar infección por virus de los equipos, fuga de información y otros riesgos que pueden afectar a la red e imagen de BEC24H.

NE08 Criptografía

PROPÓSITO

Definir requisitos de seguridad en protección de la información de BEC24H mediante criptografía.

ALCANCE

Esta norma es aplicable a todo el personal interno o terceras partes, que tenga acceso a la información de BEC24H a través de equipamiento computacional.

DOCUMENTOS DE REFERENCIA

"Estándares de Seguridad de la Información".

NORMAS

8.1 Uso de controles criptográficos

El nivel de protección de la Información debe estar basado en un análisis de riesgo, el cual identificará cuando es necesario realizar la encriptación de datos, de acuerdo al "Estándares de Seguridad de la Información" apartado "Estándar de Criptografía", el cual debe considerar Los siguientes controles:

- ✓ Restricciones de importación/exportación de hardware y software computacional para desarrollo de funciones criptográficas.
- ✓ Restricciones del uso de encriptado.
- ✓ Métodos de acceso a información encriptada (obligatorios o discrecionales) según las autoridades locales por hardware o software para proveer contenido confidencial.

8.2 Administración de llaves criptográficas

Las llaves criptográficas deben estar protegidas contra acceso y modificación no autorizada, pérdida y destrucción, de acuerdo al "Estándares de Seguridad de la Información" apartado "Estándar de Criptografía".

8.3 Encriptación de activos de información críticos

Encriptación de activos de información críticos

Los activos de información críticos si aplica, deberán ser evaluados si requerirán ser encriptados, su procedimiento de encriptación será realizado por el área de Datos de la Filial.

NE09. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

PROPÓSITO

Definir requisitos de seguridad en la adquisición, desarrollo y mantenimiento de sistemas de BEC24H.

ALCANCE

Esta norma es aplicable a todo el personal interno o terceras partes, que tenga acceso a la información de BEC24H a través de equipamiento computacional.

DOCUMENTOS DE REFERENCIA

"Estándares de Seguridad de la Información".

NORMAS

9.1 Requisitos de seguridad de los sistemas de información

9.1.1 Análisis y especificación de los requisitos de seguridad de la información

Los requerimientos para el desarrollo, actualización o adquisición de nuevos sistemas deben incluir especificaciones de seguridad de la información, según lo indicado en el "Estándares de Seguridad de la Información" apartado "Estándar de Desarrollo Seguro de Software".

9.1.2 Protección de información en redes públicas

La información de BEC24H contenida en aquellas aplicaciones que son expuestas a través de redes públicas debe contar con consideraciones de desarrollo seguro que garanticen su confidencialidad e integridad, según lo indicado en el "Estándares de Seguridad de la Información" apartado "Estándar de Desarrollo Seguro de Software".

9.1.3 Protección de transacciones en las aplicaciones

La información transaccional de las aplicaciones debe contar con mecanismos de seguridad que eviten la transmisión incompleta, el enrutamiento incorrecto, alteración, divulgación, duplicación o reproducción no autorizada.

9.2 Seguridad en los procesos de desarrollo y soporte

9.2.1 Desarrollo seguro

Todo desarrollo de software y sistemas debe considerar las reglas de seguridad descritas en el "Estándares de Seguridad de la Información" apartado "Estándar de Desarrollo Seguro de Software".

9.2.2 Control de cambios del sistema

Se debe evaluar todo cambio a los sistemas, aplicaciones o equipamiento que procese información y deben ser aprobados por la Subgerencia de Planificación y Control en conjunto con la Administración de BEC24H.

9.2.3 Revisión técnica de las aplicaciones después de los cambios en la plataforma base

Todo cambio relevante en las plataformas base de BEC24H deben implicar pruebas funcionales de las aplicaciones críticas que dependan de dichas plataformas a fin de asegurar que no se ha generado un impacto adverso en las operaciones o en la seguridad de estas.

9.2.4 Restricciones a los cambios de paquetes de software

El acceso y/o cambios a la librería de programas fuentes debe estar restringida sólo al personal autorizado.

9.2.5 Entorno de desarrollo seguro

BEC24H debe proteger adecuadamente el entorno de desarrollo en todo el ciclo de vida.

Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema (tal como Herramienta de Data analytics, entre otras) no deben estar accesibles desde los sistemas operacionales.

9.2.6 Desarrollo externalizado

BEC24H debe supervisar y monitorear toda actividad de desarrollo ejecutada por proveedores externos, a fin de garantizar que se cumplan los lineamientos definidos en "Estándares de Seguridad de la Información" apartado "Estándar de Desarrollo Seguro de Software".

9.2.7 Pruebas de seguridad del sistema

BEC24H realizará pruebas de seguridad para los desarrollos de software, de acuerdo con el "Estándares de Seguridad de la Información" apartado "Estándar de Desarrollo Seguro de Software".

9.2.8 Pruebas de aceptación de sistemas

BEC24H establecerá un programa de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones.

9.3 Datos de prueba

Los datos utilizados para la realización de pruebas se deben seleccionar cuidadosamente, proteger y controlar.

El uso de datos de producción para realizar pruebas (test y desarrollo) debe ser evaluado y autorizado conforme a los mecanismos de protección de información definidos en el "Estándares de Seguridad de la Información" apartados "Estándar de Clasificación de Activos de Información" y "Estándar de Desarrollo Seguro de Software".

9.4 Publicación de Sitios y aplicaciones Móviles

Tanto para el alojamiento de sitios externos como para la publicación de aplicaciones móviles, se deben contemplar los siguientes lineamientos:

- ✓ Todo sitio externo y/o aplicación móvil a publicar debe contar con la autorización de las áreas pertinentes.
- ✓ Todo sitio externo y/o aplicación móvil debe contar con el análisis de riesgo operacional y tecnológico respectivo, realizado en conjunto con la Gerencia de Riesgo operacional y Tecnológico, antes de publicar.
- ✓ Será responsabilidad del Ejecutivo a cargo de la implementación del sitio y/o aplicación móvil, el cumplimiento cabal de las presentes Normas Específicas de Seguridad de la Información, la "Política Integral de Riesgo Operacional y Tecnológico" y los "Estándares de Seguridad de la Información".
- ✓ Todo sitio externo y/o aplicación debe ejecutar pruebas de vulnerabilidades de seguridad que consideren la evaluación de aspectos técnicos y funcionales que pudiesen comprometer la disponibilidad, integridad y confidencialidad de la información. Estas pruebas, los resultados y las mitigaciones efectuadas deben ser informadas para revisión por la Gerencia de Ciberseguridad, antes de su paso a producción.
- ✓ Las pruebas deben ejecutarse en un entorno con condiciones equivalentes a las del ambiente de producción donde residirá el sistema.
- ✓ Los resultados de las pruebas deben quedar registrados en forma detallada por los responsables de su ejecución.

NE10. SEGURIDAD DE PROVEEDORES

PROPÓSITO

Establecer las condiciones generales que regulen la relación con terceras partes respecto a la Seguridad de la Información.

ALCANCE

Esta norma es aplicable a todas las relaciones que BEC24H mantenga con terceras partes.

DOCUMENTOS DE REFERENCIA

No hay.

NORMAS

10.1 Seguridad de la información en las relaciones con los proveedores

10.1.1 Seguridad de la información en la relación con proveedores

BEC24H incorporará en la gestión de proveedores, los requisitos de seguridad que minimicen los riesgos existentes en su ciclo de vida.

10.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores

Las relaciones con terceros que involucren el acceso de éstos a la información de BEC24H o a sus instalaciones de procesamiento, deben estar amparados en contratos formales, que incluyan cláusulas que aseguren a la filial la integridad, disponibilidad y confidencialidad de la información.

10.1.3 Cadena de suministro de la tecnología de información y comunicación

Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

10.2 Administración de prestación de servicios de proveedores

10.2.1 Monitoreo y revisión de los servicios del proveedor

BEC24H debe monitorear, revisar y auditar la prestación de servicios del proveedor de manera regular.

10.2.2 Administración de cambios en los servicios del proveedor

BEC24H considerará una reevaluación de los riesgos cada vez que existan cambios en la provisión de servicios de parte de los proveedores.

10.2.3 Amenazas o Vulnerabilidades en Servicios del proveedor

En el caso de una amenaza o vulnerabilidad de alto impacto existente en los servicios que presta el proveedor a la filial, este último tiene la potestad de cortar servicios informáticos (ej: enlaces, bajada de sistemas, etc.) en forma inmediata ante sospechas o fallas evidentes.

NE11. GESTION DE INCIDENTES

PROPÓSITO

Asegurar que los eventos de seguridad de la información y ciberseguridad y las debilidades asociadas con sistemas de información son comunicadas oportunamente con el fin tomar acciones para minimizar su impacto.

ALCANCE

Esta norma es aplicable a todo el personal interno o terceras partes, que tenga acceso a la información de BEC24H a través de equipamiento computacional.

DOCUMENTOS DE REFERENCIA

Procedimiento de Gestión de Incidentes.

NORMAS

11.1 Administración de incidentes de ciberseguridad y seguridad en la información

Entenderemos por **evento de Ciberseguridad** todas las amenazas, vulnerabilidades e incidentes de seguridad detectadas o informadas a nivel local o global, que puedan afectar a la filial o Corporación.

Se entenderá por **Incidente de Ciberseguridad**, todo evento esperado o inesperado que como consecuencia de su naturaleza, materialice el riesgo, afectando la disponibilidad o continuidad de las operaciones del Banco o sus filiales, el cual tenga como resultado una pérdida (total o parcial) de servicios, el uso indebido o afectación a la integridad de los datos o de la infraestructura tecnológica que la soporta.

Adicionalmente, se entenderá por **Amenaza de Ciberseguridad** toda condición o acción que ponga en riesgo la disponibilidad, integridad o confidencialidad de las información, sistemas o infraestructura tecnológica del Banco y sus filiales, estas amenazas pueden ser de carácter interno o externo.

Finalmente, se entenderá por **Vulnerabilidad** cualquier debilidad de un activo o control que puede ser explotada por una o más amenazas.

11.1.1 Responsabilidades y procedimientos

Las responsabilidades sobre la gestión de incidentes de seguridad de la información y ciberseguridad que permitan asegurar una respuesta oportuna y eficaz se encuentran documentadas en el "Procedimiento de Gestión de Incidentes".

11.1.2 Informe de eventos de seguridad de la información y ciberseguridad

Todos los usuarios de BEC24H deben reportar cualquier evento que pudiese comprometer la seguridad de la información, así como también cualquier vulnerabilidad que pudiese existir en los sistemas de información.

Las áreas resolutoras de incidentes de seguridad deben generar reportes periódicos a la administración señalando las situaciones más relevantes que ameriten decisiones de más alto nivel para su solución.

11.1.3 Informe de las debilidades de la seguridad de la información y ciberseguridad

Se debe instruir a los empleados y proveedores que utilizan los sistemas y servicios de información de la organización, anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios.

11.1.4 Evaluación y decisión sobre los eventos de seguridad de la información y ciberseguridad

Se deben evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información.

11.1.5 Aprendizaje de los incidentes de seguridad de la información y ciberseguridad

La información obtenida a partir de los incidentes de seguridad, debe ser utilizada para identificar y evaluar los eventos que se presenten en forma recurrente o de alto impacto y tomar las acciones correctivas según sea el caso.

11.1.6 Recopilación de evidencia

BEC24H debe establecer las acciones necesarias para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

11.2 Reportes normativos de incidentes

BEC24H debe reportar a la Comisión para el mercado financiero (CMF) los incidentes tecnológicos, incidentes de seguridad de la información e incidentes y amenazas de ciberseguridad en los siguientes reportes:

- ✓ Reporte de incidentes inmediatamente tras su ocurrencia de acuerdo a Capítulo 20-8 de la recopilación actualizada de normas.
- ✓ Reporte de incidentes y amenazas en forma mensual, en informe normativo I12, de acuerdo a lo detallado en carta circular N°6 del año 2018 de la ex Superintendencia de Bancos e Instituciones Financieras (actual Comisión para el mercado Financiero).

NE12. GESTION DE LA CONTINUIDAD

PROPÓSITO

Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas en los sistemas de información y asegurar su reanudación oportuna.

ALCANCE

Esta norma es aplicable a todo el personal interno o terceras partes, que tenga acceso a la información de BEC24H a través de equipamiento computacional.

DOCUMENTOS DE REFERENCIA

Política para la Gestión Integral del Riesgo Operacional y Tecnológico.

NORMAS

12.1 Requisitos para la continuidad del negocio

Para todos los efectos de planificación, implementación y verificación de los procesos de continuidad de negocio y su cumplimiento, se debe aplicar lo dispuesto en el ámbito de la continuidad del negocio en la "Política para la Gestión Integral del Riesgo Operacional y Tecnológico".

12.2 Disponibilidad de las instalaciones de procesamiento de la información

Las instalaciones de procesamiento de la información de BEC24H deben tener consideraciones de redundancia para cumplir con los requisitos de disponibilidad, según lo indicado en las directrices de ámbito de la continuidad del negocio en la "Política para la Gestión Integral del Riesgo Operacional y Tecnológico".

NE13. CUMPLIMIENTO NORMATIVO

PROPÓSITO

Evitar el incumplimiento de leyes, reglamentos, regulaciones o contratos.

ALCANCE

Esta norma es aplicable a todo el personal interno o terceras partes, que tenga acceso a la información de BEC24H a través de equipamiento computacional.

DOCUMENTOS DE REFERENCIA

Política para la Gestión Integral del Riesgo Operacional y Tecnológico.

NORMAS

13.1 Cumplimiento con los requisitos legales y contractuales

13.1.1 Identificación de los requisitos de legislación y contractuales correspondientes

Todos los requisitos estatutarios, normativos y contractuales legislativos en lo que respecta a seguridad de la información y ciberseguridad, y el enfoque de BEC24H para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.

13.1.2 Derechos de propiedad intelectual

BEC24H debe implementar procedimientos para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual.

Los contratos, certificados o cualquier otro elemento que compruebe la propiedad de BEC24H sobre el software utilizado en sus sistemas, debe mantenerse adecuadamente custodiado.

13.1.3 Protección de registros

De acuerdo con los requisitos legislativos, normativos, contractuales y comerciales, los registros de BEC24H se deben proteger contra pérdida, destrucción, falsificación, acceso y publicación no autorizada.

BEC24H debe mantener respaldo de la información de sus operaciones por un lapso de tiempo que asegure el cumplimiento del requerimiento legal establecido en esta materia.

13.1.4 Privacidad y protección de información personal identificable

BEC24H debe garantizar la confidencialidad e integridad de la información personal identificable conforme a lo indicado en la legislación y las normativas correspondientes.

13.2 Revisiones de la seguridad de la información

13.2.1 Revisión independiente de la seguridad en la información

BEC24H debe efectuar periódicamente una revisión independiente de su gestión en seguridad de la Información, que considere la revisión de sus políticas, estándares y procedimientos y su implementación.

13.2.2 Cumplimiento con las políticas y normas de seguridad

Los Gerentes deben revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad con las políticas, normas y cualquier otro tipo de requisitos de seguridad correspondientes.

13.2.3 Revisión de cumplimiento técnico

Los sistemas de información de BEC24H deben someterse periódicamente a revisiones técnicas de seguridad para verificar el cumplimiento de la "Política para la Gestión Integral del Riesgo Operacional y Tecnológico".

NE14. CIBERSEGURIDAD

PROPÓSITO

Asegurar la confidencialidad, integridad y disponibilidad de los activos de información digital, y cumplir con las Leyes y Reglamentaciones vigentes en cada momento, manteniendo un equilibrio entre los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

ALCANCE

Esta norma es aplicable a todo el personal interno o terceras partes, que tenga acceso a la información de BEC24H a través de equipamiento computacional.

DOCUMENTOS DE REFERENCIA

Política para la Gestión Integral del Riesgo Operacional y Tecnológico.

NORMAS

14.1 Gestión de la Ciberseguridad

Todas las normas antes expuestas desde Organización de la Seguridad hasta Cumplimiento con los requisitos legales y contractuales son aplicables para la Gestión de la Ciberseguridad.

14.2 Metodología de Gestión de la Ciberseguridad

BEC24H debe implementar una metodología que permita mantener niveles adecuados de Ciberseguridad.

14.3 Proceso de Gestión de la Ciberseguridad

BEC24H debe implementar un proceso que permita mantener niveles adecuados de Ciberseguridad. Este proceso debe contemplar las etapas de identificación, protección, detección, respuesta y recuperación.

14.3.1 Etapa de Identificación

La etapa de identificación, debe considerar lo siguiente:

- ✓ Manejo de activos
- ✓ Ambiente de negocio
- ✓ Modelo de Gobierno
- ✓ Evaluación de riesgos
- ✓ Estrategia de administración del riesgo (mitigar, transferir, prevenir o aceptar)
- ✓ Gestión de riesgos de los procesos.

Lo anterior, en cumplimiento de las normas NE03 "Clasificación y Control de Activos de Información", NE01 "Organización de la Seguridad" y de acuerdo a las metodologías y escala de evaluación de riesgo operacional y tecnológico de BEC24H.

14.3.2 Etapa de Protección

La etapa de protección, debe considerar lo siguiente:

- ✓ Control de acceso y gestión de identidades.
- ✓ Conciencia y entrenamiento.
- ✓ Seguridad de datos
- ✓ Procesos y procedimientos de protección de información
- ✓ Mantención
- ✓ Tecnología de protección.

Lo anterior, en cumplimiento de las normas NE04 "Control de Acceso", NE02 "Seguridad en los recursos humanos", NE06 "Seguridad de las Operaciones", NE07 "Seguridad de las Comunicaciones" y NE08 "Criptografía".

14.3.3 Etapa de Detección

La etapa de detección, debe considerar lo siguiente:

- Detección de eventos y anomalías
- Monitoreo continuo de seguridad
- Procesos de detección

Lo anterior, en cumplimiento de la norma NE11 "Gestión de Eventos, Incidentes y Amenazas".

14.3.4 Etapa de Respuesta

La etapa de respuesta, debe considerar lo siguiente:

- Plan de respuesta frente a eventos, incidentes y amenazas
- Comunicación de incidentes y amenazas
- Análisis de eventos, incidentes y amenazas
- Mitigación de eventos, incidentes y amenazas
- Mejora continua

Lo anterior, en cumplimiento de la norma NE11 "Gestión de Eventos, Incidentes y Amenazas".

14.3.5 Etapa de Recuperación

La etapa de recuperación, debe considerar lo siguiente:

- Plan de recuperación
- Mejora continua
- Conciencia y comunicación

Lo anterior, en concordancia con el DRP de BancoEstado (Plan de recuperación de desastres) y en cumplimiento de las normas: NE11 "Gestión de Eventos, Incidentes y Amenazas", NE12 "Gestión de la Continuidad".

14.4 Gestión de Incidentes de Ciberseguridad

BEC24H debe diseñar e implementar un protocolo que permita gestionar la respuesta ante incidentes de Ciberseguridad.