POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

La información es un activo de valor crítico para NOFRAUD. Los empleados y todos aquellos que tienen responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de NOFRAUD deben adoptar los lineamientos contenidos en el presente documento, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la misma, así como minimizar los riesgos a los que se encuentra expuesta dicha información. La política global de seguridad de la información de NOFRAUD está soportada por directrices, normas y procedimientos específicos los cuales orientan sobre el manejo adecuado de la información de la empresa.

1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Las políticas específicas de seguridad de la información de NOFRAUD se fundamentan en los dominios y objetivos de control de la norma ISO/IEC 27001:2013 y se enuncian a partir de este numeral. Las políticas y normas de seguridad de la información son aplicables, de manera general, a todos los empleados, contratistas y empleados en misión de la empresa.

1.1 PREMISAS

La dirección ejecutiva de NOFRAUD mantendrá un compromiso permanente con la seguridad de la información.

1.2 POLÍTICA

La Dirección Ejecutiva de NOFRAUD se comprometerá a aprobar el presente documento de políticas de seguridad de la información. De la misma manera, lo deberá revisar y ajustar de manera periódica para mantener la vigencia de éstas, así como a garantizar su divulgación y cumplimiento de todos los empleados, contratistas y empleados en misión. Como parte de su compromiso designará a los entes encargados de la seguridad de la información al interior de la empresa. La Dirección Ejecutiva debe aprobar las políticas de seguridad de la información, demostrando así su compromiso con la seguridad de la información en NOFRAUD, una vez aprobadas, debe velar por su divulgación y cumplimiento al interior de la empresa. Se deben definir y asignar responsabilidades a cada uno de los roles que desempeñarán un papel en la gestión de la seguridad de la información en todos los niveles de la empresa. La Dirección Ejecutiva debe revisar periódicamente la aplicabilidad y vigencia de las políticas de seguridad de la información y efectuar los ajustes necesarios sobre ellas para que sean funcionales y se pueda seguir exigiendo su cumplimiento por parte de todos los empleados, contratistas y empleados en misión de la empresa.

2 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

2.1 ORGANIZACIÓN INTERNA

2.1.1 PREMISA

La organización de seguridad de la información debe establecerse y mantenerse acorde con las necesidades de NOFRAUD y las mejores prácticas con el fin de implantar y gestionar el proceso de seguridad de la información.

2.1.2 POLÍTICA

En la implementación de un sistema de gestión de seguridad de la información efectivo se debe garantizar que existan tres elementos fundamentales: organización, procesos y tecnología. La organización de seguridad de la información consiste en la generación de capacidad de gestión proactiva que pueda reaccionar en forma oportuna a las nuevas necesidades de protección de la información en congruencia con las metas y objetivos de NOFRAUD.

2.1.3 NORMAS

Dentro de la organización interna de seguridad de la información se identificarán roles a saber: custodio, usuario o propietario de la información, cada rol debe identificar, analizar, evaluar, tratar y monitorear el cumplimiento de la política.

El uso de los recursos de información de NOFRAUD por personal que no pertenece a la empresa ya sea local o remotamente, debe ser formalizado por medio de acuerdos que hagan obligatorio el cumplimiento de la presente política.

2.2 TERCEROS

2.2.1 PREMISA

Los terceros que efectúen el tratamiento de información propia de NOFRAUD o sobre la cual la empresa sea responsable, deben cumplir con la política junto con su sistema de gestión empresarial en sus prácticas de seguridad de la información.

2.2.2 POLÍTICA

Los contratos, convenios y órdenes de servicios que celebre NOFRAUD deben incluir cláusulas que especifiquen las responsabilidades sobre el adecuado tratamiento de información, de acuerdo a las disposiciones legales vigentes sobre el tema. Se debe mantener un registro por contratista, proveedor, cliente y usuario del entendimiento y seguimiento de la política, en atención a los lineamientos dados por la dirección de tecnología.

2.2.3 NORMAS

A. Se debe incluir las cláusulas de confidencialidad y buen tratamiento de la información (protección de datos) dentro de los contratos, convenios y órdenes de servicios que realice la empresa.

B. De igual forma se debe incluir un acuerdo formal de niveles de servicios en seguridad de la información, en el que se detallen los compromisos en el cuidado de los recursos de información de NOFRAUD y las sanciones en caso de incumplimiento. El cumplimiento de los niveles de servicios en seguridad de la información de terceros debe ser verificado y controlado permanentemente por quienes ejerzan las funciones de supervisión de los contratos suscritos por NOFRAUD. Cuando la interventoría sea contratada, se debe incluir esta obligación dentro de los contratos. En el caso en que la supervisión sea realizada por empleados de NOFRAUD, se entiende que el

cumplimiento de la política está incorporado dentro de sus obligaciones como empleado y como supervisor.

3 GESTIÓN DE ACTIVOS

3.1 RESPONSABILIDAD SOBRE LOS ACTIVOS

3.1.1 PREMISAS

Cada activo de información de NOFRAUD debe tener asignado un responsable, quien debe preservar el cumplimiento de las características de la información señaladas en los objetivos de la política. Los recursos de información son provistos a los usuarios para uso exclusivo y excluyente de los fines con los cuales le fue entregada y/o permitido su acceso por parte del responsable.

3.1.2 POLÍTICA

La información que NOFRAUD utilice para el desarrollo de sus objetivos tiene asignado un responsable, quién la utiliza y es el que responde por su correcto tratamiento. Así toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de tratamiento. Cada responsable debe conocer la información que debe cuidar, vigilar su correcto tratamiento, los lugares donde reside y los usuarios de la misma. Dichos usuarios deben demostrar una necesidad de negocio para su acceso, el cual debe ser vigilado por el responsable.

3.1.3 NORMAS

A. La información provista por los clientes, accionistas, proveedores, terceros, asociados, empleados, contratistas y empleados en misión, es privada y su tratamiento dentro de las premisas de NOFRAUD está enmarcado para los fines que fue obtenida.

B. NOFRAUD debe proveer los medios necesarios para asegurarse que cada usuario preserve y proteja los activos de información de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer o sobrepasar cualquier control de seguridad de la información en forma no autorizada será sujeto de las acciones legales correspondientes.

C. Los recursos de información de NOFRAUD son exclusivamente para propósitos de la empresa y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Los empleados que intenten acceder a información para la cual no están autorizados, incurrirán en violación de la política.

D. Se debe promover el buen uso de los recursos de información, conservando el derecho a la intimidad, la privacidad, el habeas data, y la protección de los datos de sus propietarios. En consecuencia, se deberán crear registros de las actividades realizadas, que puedan ser revisados con el objetivo de detectar abusos y/o amenazas sobre la información.

E. NOFRAUD se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente.

4 CLASIFICACIÓN DE LA INFORMACIÓN

4.1 PREMISAS

El responsable de la información debe clasificarla, basado en la sensibilidad, valor, riesgo de pérdida o compromiso de la misma y/o requerimientos legales. La información de NOFRAUD es un activo estratégico, por lo tanto, debe ser protegida permanentemente.

NOFRAUD realiza el tratamiento de la información de terceros sobre la cual es responsable, con el mismo grado de diligencia con que realiza el tratamiento de su propia información.

4.2 POLÍTICA

Toda la información de NOFRAUD debe estar clasificada por el responsable de la información con base en un análisis de alto nivel del impacto al negocio en seguridad de la información; que determine su valor relativo, su privacidad y nivel de riesgo a que está expuesta.

4.3 NORMAS

A. Los niveles de clasificación de la información se deben realizar con base en su sensibilidad, valor, riesgo de pérdida o compromiso, y/o requerimientos legales de retención. Dichos niveles serán divulgados y oficializados a los usuarios de la información para asegurar que los niveles de protección son entendidos y se mantienen a través de la empresa.

B. Cada nivel de clasificación tendrá un conjunto de controles determinados por NOFRAUD, los que podrán ser complementados y aumentados, nunca disminuidos, por el responsable de la información con la ayuda de seguridad de la información. Estos serán diseñados para proveer un nivel de protección de la información apropiado y consistente dentro de la empresa, sin importar el medio, formato o lugar donde se encuentre, deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

C. Si la información clasificada de NOFRAUD debe ser entregada a contratistas, asociados y terceros por efectos del proceso, previamente se deben firmar los acuerdos de confidencialidad respectivos, que incluyan el seguimiento y cumplimiento de las prácticas de gestión segura de la información al tenor de lo establecido en la política. Igualmente si la información clasificada de la empresa es requerida por algún ente externo o ciudadano en donde opere NOFRAUD, su entrega estará supeditada a la aprobación previa de su responsable y de las instancias establecidas.

5 SEGURIDAD DEL PERSONAL

5.1 PREMISAS

NOFRAUD establecerá un programa permanente de capacitación y transformación de la cultura en seguridad de la información.

NOFRAUD proveerá los mecanismos necesarios que le permitan a los usuarios cumplir con sus responsabilidades en seguridad de la información desde su vínculo inicial hasta que cesen sus compromisos con la empresa.

NOFRAUD en cabeza del comité de seguridad de la información debe contar con un programa permanente de creación de cultura en seguridad de la información con medidas de protección y/o controles, que permita asegurar que los destinatarios de la política conozcan y entiendan sus responsabilidades en seguridad de la información, así como, sobre las continuas amenazas que ponen en riesgo la información que manejan.

5.2 POLÍTICA

Como parte del programa de capacitación en seguridad de la información, el personal que ingrese vinculado de manera temporal y/o indefinidamente a NOFRAUD deberá asistir de manera obligatoria durante su inducción, a las charlas que sobre los requerimientos de seguridad de la información se dicten. Todos los empleados, contratistas y empleados en misión de la empresa tendrán acceso permanente a la política y se obligan a cumplirla.

5.3 NORMAS

A. En los procesos de selección, reclutamiento, incorporación, estadía y cierre de contrato de empleados de NOFRAUD, deberá pasar por un proceso de selección con la investigación adecuada, con el fin de mitigar los riesgos en el tratamiento de la información de NOFRAUD. El grado de investigación dependerá del nivel de sensibilidad que tiene la posición del empleado dentro de la empresa y el contacto que estos tendrán con la información. Los criterios para definir el nivel de investigación serán establecidos por la dirección administrativa.

B. Para los empleados que en su proceso de vinculación con NOFRAUD, no hayan recibido capacitación básica en seguridad de la información, se programará la re-inducción que cubra los aspectos más relevantes y de conocimiento general para todos los empleados.

6 POLÍTICA DE SEGURIDAD FÍSICA Y EL ENTORNO

6.1 PREMISAS

NOFRAUD deberá proveer instalaciones que permitan procesar la información de la empresa de manera segura, y facilitar que sus empleados realicen las actividades diarias en óptimas condiciones.

6.2 POLÍTICA

NOFRAUD garantizará entornos con controles de acceso idóneos, los cuales asegurarán el perímetro, tanto en oficinas, recintos, áreas de carga y descarga, así como en entornos abiertos para evitar el acceso no autorizado a ellos. Del mismo modo, controlará las amenazas físicas externas y velará por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información documentales.

Así mismo, deberá exigir a sus terceros para que estos, a su vez, exijan al proveedor de servicios de centro de cómputo el cumplimiento de la implementación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con que éste debe contar.

6.3 NORMAS

6.3.1 ÁREAS SEGURAS

A. El ingreso de terceros a los centros de cableado, debe estar debidamente registrado mediante una bitácora ubicada en un lugar visible a la entrada de estos lugares.

B. Los privilegios de acceso físico a los centros de cableado deben ser descontinuados o modificados oportunamente a la terminación, transferencia o cambio en las labores de un empleado autorizado.

C. Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas cuando los empleados se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.

D. Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizados por los empleados autorizados y, salvo situaciones de emergencia, estos no deben ser transferidos a otros empleados, contratistas y empleados en misión de la empresa.

E. Las oficinas e instalaciones donde se maneje información sensible deben contar con sistemas de alarmas y cámaras.

F. Todos los empleados, contratistas y empleados en misión deben permanecer con el carné que los identifica como empleados de NOFRAUD, mientras permanezcan en las instalaciones de la empresa.

G. Todos los empleados, contratistas y empleados en misión deben reportar a la dirección administrativa, a la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación y tarjetas de acceso físico a las instalaciones de la compañía.

H. Los empleados, contratistas y empleados en misión de NOFRAUD no deben intentar ingresar a áreas a las cuales no tengan la debida autorización.

I. Todos los visitantes que ingresan a la empresa, deben ser recibidos y estar acompañados por la persona a quien visitan durante su permanencia en las instalaciones de la misma.

J. La documentación física generada, recibida y en general, manipulada por los empleados, contratistas y empleados en misión de la empresa debe estar ubicada en archivos o repositorios con condiciones de temperatura y humedad adecuadas, de acuerdo con las directrices de la función archivística de la institución ó gestión documental.

6.3.2 SEGURIDAD DE LOS EQUIPOS

A. El centro de cómputo debe contar con mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas o controles biométricos que la compañía encargada de prestar este servicio considere críticas.

B. El ingreso de terceros al centro de cómputo debe estar debidamente registrado mediante una bitácora ubicada en un lugar visible a la entrada estos lugares.

C. Los ingresos al centro de cómputo deben ser monitoreados regularmente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.

D. El centro de cómputo debe estar separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.

E. Deben existir mecanismos de revisión y control del ingreso de cualquier tipo de material al centro de cómputo.

F. En el centro de cómputo deberán existir sistemas de detección y extinción automáticas de incendios, control de inundación y alarmas en caso de detectarse condiciones inapropiadas.

G. Los niveles de temperatura y humedad relativa en el centro de cómputo deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado.

H. Se debe monitorear de manera permanente el estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte del centro de cómputo, como son el sistema de aire acondicionado y el sistema de detección y extinción de incendios, entre otros.

I. Los trabajos de mantenimiento de redes eléctricas, cableado de datos y voz, deben ser realizados por el personal especialista y debidamente autorizado e identificado.

J. Se deben realizar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS y/o plantas eléctricas, de los sistemas de detección y extinción de incendios y del sistema de aire acondicionado.

K. Se deben configurar y monitorear los equipos que manejan información crítica del negocio para que estén perfectamente integrados al sistema UPS y dado el caso de que la planta del edificio falle y las baterías se agoten, poder apagar de forma automática y controlada cada uno de los sistemas, atendiendo a la premisa de salvaguardar la integridad de la información.

L. Se deben realizar mantenimientos preventivos de los servidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de NOFRAUD.

M. Se debe proveer un procedimiento, que garantice la realización del mantenimiento de las estaciones de trabajo y equipos portátiles, así como su adecuación para la reutilización o reasignación de manera segura en el cual se conserve la disponibilidad, integridad y confidencialidad de la información contenida en los mismos.

N. La Dirección de Tecnología debe garantizar la adopción de los controles necesarios para asegurar que los suministros de electricidad, así como las redes de comunicaciones se encuentran protegidos.

7 POLÍTICAS DE GESTIÓN DE LAS OPERACIONES Y LAS COMUNICACIONES

7.1 PREMISAS

La información de NOFRAUD debe preservar su nivel de protección cuando esta se transmita a través de redes diferentes a la red privada de la empresa.

7.2 POLÍTICA

La Dirección de Tecnología de NOFRAUD, encargada de la operación y administración de la plataforma tecnológica que apoya los procesos de negocio, asignará funciones específicas a sus empleados quienes actuarán como responsables de garantizar la adecuada operación y administración de dicha plataforma, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de dichas actividades.

7.3 NORMAS

A. Los responsables de la seguridad de la información deben apoyar en la definición de soluciones para dar cumplimiento a los niveles de seguridad establecidos en NOFRAUD.

B. Se debe garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio de NOFRAUD.

C. Se deben establecer responsabilidades y procedimientos que aseguren una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información que se llegasen a presentar en la empresa.

D. La Dirección de Tecnología debe proveer a sus empleados de manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información, para toda la plataforma tecnológica de la empresa.

8 CONTROL DE CAMBIOS

8.1 POLÍTICA

NOFRAUD establecerá, coordinará y controlará los cambios realizados en los activos de información tecnológicos y los recursos informáticos, asegurando que los cambios efectuados

sobre la plataforma tecnológica, tanto el software operativo como los sistemas de información, serán adecuadamente controlados y debidamente autorizados por las áreas correspondientes. Cualquier tipo de cambio quedará formalmente documentado desde su solicitud hasta su implementación.

8.2 NORMAS

A. Se debe documentar, establecer, publicar y poner en operación un procedimiento de control de cambios tanto para software de base como para las aplicaciones de NOFRAUD.

B. Se debe establecer responsabilidades y procedimientos para controlar los cambios en los activos de información, recursos informáticos y en el software de la compañía.

C. La Dirección de Tecnología debe garantizar que todo cambio realizado a un componente de la plataforma tecnológica, el cual conlleve modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes.

D. Se debe garantizar que todo cambio realizado sobre la plataforma tecnológica de NOFRAUD quedará formalmente documentado desde su solicitud hasta su implementación cumpliendo con el procedimiento correspondiente.

E. La Dirección de Tecnología debe proveer los recursos necesarios que garanticen la separación de ambientes de desarrollo, pruebas y producción, así como de la independencia de los empleados que ejecutan dichas labores.

F. Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.

G. Los dueños o responsables deben proveer los recursos necesarios que garanticen la realización de pruebas suficientes de funcionalidad y operación, las cuales deben ser documentadas y aprobadas formalmente con los cambios solicitados.

H. Los administradores de los activos de información tecnológicos y recursos informáticos deben garantizar que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios, siguiendo el procedimiento vigente para dicha acción.

I. Todos los usuarios de activos de información tecnológicos y recursos informáticos que requieran la adición o modificación de funcionalidades de los mismos, deben solicitar dicho cambio por medio del procedimiento vigente para dicha acción.

9 PLANEACIÓN Y ACEPTACIÓN DE SISTEMAS DE INFORMACIÓN

9.1 POLÍTICA

La Dirección de Tecnología de NOFRAUD será la responsable de realizar las proyecciones de crecimiento y provisiones de la plataforma tecnológica, de manera periódica, con el fin de

garantizar la correcta operación de los recursos informáticos y sistemas de información que apoyan los procesos de la empresa.

9.2 NORMAS

A. La Dirección de Tecnología debe garantizar que antes de seleccionar y poner en producción un recurso informático, ha realizado el correcto estudio sobre la demanda y las proyecciones de crecimiento del recurso (capacity planning) para asegurar el desempeño y la capacidad de almacenamiento.

B. La Dirección de Tecnología debe garantizar que la puesta en producción de los sistemas de información, productos y/o servicios estarán precedidas por la ejecución y aprobación del programa o plan de pruebas.

10 PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

10.1 POLÍTICA

NOFRAUD proveerá los recursos necesarios que garanticen la protección de la información y los recursos de procesamiento de la misma adoptando controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por la contaminación y/o el contagio de software malicioso.

10.2 NORMAS

A. La Dirección de Tecnología debe proveer recursos informáticos y software tales como antivirus, antimalware, detectores de intrusos, software antispam entre otros, los cuales garanticen la seguridad de la información contenida, gestionada y administrada en los activos de información tecnológicos y servicios que se ejecuten sobre los mismos.

B. La Dirección de Tecnología debe garantizar que los activos de información, así como, los recursos tecnológicos son actualizados periódicamente, evitando que código malicioso y virus ejecuten vulnerabilidades del sistema de los mismos.

C. La Dirección de Tecnología debe garantizar que el software usado para la mitigación de virus informáticos cuenta con las licencias de uso aprobadas, garantizando su autenticidad y su periódica actualización tanto de la versión de la aplicación como de la base de datos de virus reconocidos.

D. La Dirección de Tecnología debe garantizar que la información almacenada en los activos de información tecnológicos que es transportada por la red de datos, es escaneada con una periodicidad establecida para garantizar así la seguridad de la misma.

E. La Dirección de Tecnología debe garantizar que los usuarios de los activos de información tecnológicos no pueden modificar la configuración establecida para el software antivirus.

F. Los usuarios de activos de información tecnológicos y recursos informáticos deben hacer uso exclusivo de hardware y software autorizados por los empleados de La Dirección de Tecnología.

G. Los usuarios de activos de información tecnológicos y recursos informáticos deben garantizar que las descargas de archivos adjuntos de los correos electrónicos o descargados de Internet realizadas provienen de fuentes conocidas, seguras y exclusivas de acuerdo con las funciones encomendadas.

H. Los usuarios de activos de información tecnológicos y recursos informáticos deben correr el software antivirus sobre archivos y/o documentos que son abiertos y/o ejecutados por primera vez.

I. Los usuarios de activos de información tecnológicos deben comunicarse con La Dirección de Tecnología al encontrar un virus, del cual no se sabe cómo eliminarlo, cómo actuar frente al mismo o de considerarlo necesario.

J. Los empleados, contratistas y empleados en misión deben cumplir con estos cuidados a cabalidad, es así, que todos los terceros que usen equipos propios o de sus contratantes deben mantener instalado y funcionando el software antivirus.

K. La Dirección de Tecnologías debe tener y mantener un procedimiento de atención de incidentes de seguridad especializado en la detección y tratamiento de malware, que implique una fuga o exposición de información sensible a personas no autorizadas.

11 ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN

11.1 POLÍTICA

Los empleados responsables de la gestión del almacenamiento y respaldo de la información deberán proveer los recursos necesarios para garantizar el correcto tratamiento de la misma. Las áreas encargadas de la información en conjunto con La Dirección de Tecnología deberán definir la estrategia a seguir para el respaldo y almacenamiento de la información.

11.2 NORMAS

A. Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben definir en compañía de La Dirección de Tecnología estrategias para la correcta y adecuada generación, retención, y rotación de las copias de respaldo de la información.

B. Los dueños o responsables de los activos de información tecnológicos y recursos informáticos deben velar por el cumplimiento de los procedimientos de respaldo de la información.

C. La Dirección de Tecnología debe establecer lineamientos para la generación y almacenamiento de las copias de respaldo.

D. La Dirección de Tecnología debe proveer procedimientos para la correcta y segura generación, así como el adecuado tratamiento de las copias de respaldo.

E. La Dirección de Tecnología debe contar con procedimientos e infraestructura disponible para realizar pruebas a las copias de respaldo para garantizar su integridad y usabilidad en caso de ser requerido.

F. Los administradores de los activos de información tecnológicos y recursos informáticos deben almacenar y respaldar las copias de seguridad según el procedimiento vigente de NOFRAUD, de tal forma que se garantice su confidencialidad, integridad y disponibilidad.

G. Los administradores de los activos de información tecnológicos y recursos informáticos deben ejecutar los procedimientos provistos por La Dirección de Tecnología para realizar pruebas a las copias de respaldo.

H. Los administradores de los activos de información tecnológicos y recursos informáticos deben realizar pruebas periódicas de recuperación de la información respaldada y documentar sus resultados.

12 INTERCAMBIO DE INFORMACIÓN

12.1 POLÍTICA

NOFRAUD en su intención de proteger la información de la empresa, indistintamente del lugar o forma en la que esta se encuentre almacenada, proveerá los recursos necesarios para garantizar la protección de la misma al momento de ser transferida, comunicada a un tercero o al salir de sus instalaciones según necesidad de la actividad o proceso particular.

12.2 NORMAS

A. Los responsables del intercambio de información con entidades externas deben definir en compañía de La Dirección de Tecnología las estrategias para la correcta gestión e intercambio seguro de la misma.

B. Los responsables del intercambio de información con entidades externas deben diseñar, establecer y aplicar acuerdos en los cuales se definan las responsabilidades en el intercambio de información de las partes que interactúen en el mismo.

C. La Dirección de Tecnología debe proveer los recursos necesarios con los cuales sea posible garantizar el correcto, adecuado y seguro intercambio de información desde estaciones de trabajo y equipos portátiles, así, como desde los dispositivos externos o móviles. Así mismo, debe garantizar que las transacciones de NOFRAUD realizadas de manera electrónica o haciendo uso de las redes de comunicaciones y las estaciones de trabajo de la misma, cuentan con los controles suficientes para evitar transmisiones incompletas, enrutamiento no apropiado o erróneo, repeticiones de las mismas no autorizadas, perdida de confidencialidad, integridad de las mismas y perdida de disponibilidad del servicio.

D. Los administradores de los activos de información tecnológicos y recursos informáticos deben aplicar los controles necesarios que garantizan la disponibilidad, confidencialidad e integridad de la información transmitida electrónicamente por

medio de recursos tecnológicos de propiedad o provistos por la empresa, según necesidad o el nivel de criticidad de la misma.

E. Los administradores de los activos de información tecnológicos y recursos informáticos deben garantizar que las estaciones de trabajo y/o dispositivos móviles utilizados en procesos de banca electrónica cuentan con los controles necesarios para la realización de pagos y transacciones de manera segura.

F. Los usuarios empleados, contratistas y empleados en misión que interactúen en procesos de intercambio de información al exterior de la empresa deben cumplir los lineamientos, recomendaciones y/o estrategias establecidas para este propósito en NOFRAUD.

13 GESTIÓN Y USO ADECUADO DE INTERNET

13.1 POLITICA

La información clasificada de NOFRAUD no puede viajar sobre redes externas. Cuando exista una razón justificada de negocio y por medio de un manejo de riesgo aprobado por el responsable de la información que de paso a medidas de protección como cifrado, firmas digitales, procedimientos de uso y tratamiento de información clasificada y otras que sean requeridas; se pueden realizar transferencia de datos y archivos hacia redes externas incluida Internet.

Para evitar la fuga de información, la empresa debe impedir la transferencia de archivos o información hacia redes externas incluidas Internet sin la autorización del responsable de la información. Para el envío de información clasificada de la empresa se debe mantener su nivel de confidencialidad y se deben tomar las medidas de seguridad que salvaguarden su integridad.

13.2 NORMAS

A. Los usuarios de NOFRAUD para acceder a servicios de Internet e Intranet son absolutamente responsables de la utilización que hagan de dichos servicios y por las consecuencias que se deriven de su utilización.

B. En el momento que NOFRAUD autorice y provea las facilidades para el acceso a servicios de Internet/Intranet a un usuario, este debe tener pleno conocimiento de la política y normas de seguridad de la información establecidas por la empresa y que regulan la conducta de todo usuario frente a la utilización de los elementos de tecnología. El uso que el usuario haga de los servicios de Internet/Intranet en la empresa debe estar alineado con el sistema de gestión en seguridad de la información y debe satisfacer una necesidad legítima de la misma.

C. El acceso de usuarios a los servicios de Internet debe ser autorizado únicamente para satisfacer una necesidad legítima de la misión de la empresa, en el desempeño de sus responsabilidades.

D. Se debe implementar un programa de verificación periódica de autorizaciones de acceso a Internet, cuyo objetivo sea bloquear el acceso a usuarios que ya no cuenten

con una justificación válida de la empresa para acceder a este servicio. De igual forma los requerimientos sobre la restricción de acceso de un usuario a Internet deben ser tramitados inmediatamente sean solicitados.

E. La Dirección de Tecnología deberá buscar y controlar el uso no autorizado de canales de acceso a internet externos a NOFRAUD (rogue access points), tales como MIFI, Planes de datos celulares y routers 4G LTE, que le permitan a un empleado de la empresa conectar su equipo de trabajo, acceder a internet y vurlar los controles de seguridad para la navegación segura.

14 POLÍTICAS DE CONTROL DE ACCESO

14.1 PREMISAS

Cada usuario que accede a la información de NOFRAUD debe disponer de un medio de identificación y su acceso debe ser controlado a través de una autenticación personal.

El tratamiento de la información de NOFRAUD debe ser dado, mantenido y controlado con base en una necesidad de negocio demostrada.

14.2 POLÍTICA

Los usuarios de NOFRAUD serán requeridos para que se autentiquen ellos mismos previa obtención del acceso a la información. Dependiendo del valor y de la privacidad de la Información, al igual que el nivel de riesgo, NOFRAUD definirá medios de identificación y autenticación apropiados, que no podrán ser compartidos y deberán estar habilitados solamente para los recursos de información acordados y establecidos por NOFRAUD. Dichos medios de autenticación contienen información clasificada que no debe ser revelada o almacenada en lugares que puedan ser accedidos de manera no autorizada.

14.3 NORMAS

A. Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de NOFRAUD. Por lo tanto, la identidad de cada usuario de los recursos de información deberá ser establecida y autenticada de una manera única. Esta de ninguna manera o por ninguna circunstancia podrá ser compartida.

B. Previo al acceso a un activo de información cada usuario debe demostrar su identidad utilizando el medio establecido, autorizado y provisto por NOFRAUD. El sobrepaso a este medio será tratado como una infracción a la seguridad de la información.

C. Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que los activos de información de la empresa se mantengan protegidos de una manera consistente con su valor para el negocio y con los riesgos de pérdida de integridad, confidencialidad, disponibilidad y confiabilidad de la información.

D. Los niveles de acceso deben reflejar permanentemente una necesidad clara y demostrada de negocio y no deben comprometer la segregación de funciones y responsabilidades.

E. El acceso a la información de NOFRAUD deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad o tipo de servicio. El acceso a los recursos de información de NOFRAUD debe ser restringido en todos los casos sin excepción, y se debe dar específicamente a quienes lo requieran en razón de sus funciones, con los privilegios apropiados y por un tiempo limitado.

F. Los niveles de acceso deben ser revisados periódicamente por el respectivo responsable de la información y cualquier desviación será tratada como un incidente en seguridad de la información. Los responsables deben dejar trazas del ejercicio de esta actividad, las que serán objeto de revisiones de parte de NOFRAUD.

G. El uso remoto de los activos de información y la computación móvil será realizado bajo una autorización previa de los responsables de la información, junto con su respectivo manejo de riesgo aprobado por NOFRAUD.

H. El acceso a cada uno de los ambientes debe ser controlado y exclusivo conforme lo establece los roles de la empresa. Ningún rol puede tener acceso a más de uno de estos.

I. Se deben establecer controles físicos y de acceso lógico para los ambientes de desarrollo, pruebas y producción de los activos de Información de NOFRAUD para que permanezcan completamente separados.

J. El acceso a la información en producción de NOFRAUD debe hacerse únicamente por los aplicativos y sistemas autorizados. En ningún caso la información puede ser accedida directamente.

K. Si entes externos tienen acceso a información crítica de NOFRAUD, se deben suscribir acuerdos para la salvaguardar de la misma. La información de NOFRAUD que está en manos de personas externas debe tener el mismo o mayor nivel de protección como si estuviera administrada por la empresa, por lo cual es necesario efectuar revisiones a fin de conocer cómo se está manejando y protegiendo la información externamente.

15 POLÍTICAS PARA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

15.1 PREMISAS

Cada solución que se implemente en NOFRAUD, debe incluir los requerimientos de seguridad de la información, durante su ciclo de vida.

15.2 POLÍTICA

Los responsables por la provisión de soluciones deben crear y mantener una metodología que controle el ciclo completo de adquisición, desarrollo, mantenimiento y disposición seguro de soluciones de información e infraestructura.

15.3 NORMAS

A. Los requerimientos de seguridad de la información deben ser identificados previos al diseño o requisición de soluciones de información e infraestructura. De ser necesario el desarrollo interno, los requerimientos deben ser incluidos dentro de los sistemas y si una modificación es solicitada, debe cumplir estrictamente con los requerimientos de seguridad de la información que han sido previamente establecidos.

B. La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección ni ser utilizada en ambientes de desarrollo y pruebas, tanto para mantenimiento como el desarrollo de soluciones.

C. La información tratada por las aplicaciones aceptadas por NOFRAUD debe preservar su confiabilidad desde su ingreso, transformación y entrega al negocio. Cada aplicación válida que se use y/o transforme información del negocio debe establecer los medios que preserven su integridad y confidencialidad.

D. Cada solución de información o de infraestructura debe mantener durante su ciclo de vida una gestión de riesgo que informe permanentemente el nivel de exposición que representa para NOFRAUD.

E. Cualquier cambio en el ciclo de vida de un elemento de la plataforma de operación de NOFRAUD debe seguir los procesos de control de cambios y acreditación de la instalación, para que preserve el cumplimiento de la política.

16 POLÍTICAS PARA LA GESTIÓN DE INCIDENTES

16.1 PREMISA

NOFRAUD vigilará permanentemente el cumplimiento de la presente política y cuando exista una violación será alertada en el mismo instante a las instancias oficiales establecidas para tal fin.

16.2 POLÍTICA

Las situaciones o acciones que violen la presente política deben ser detectadas, registradas, analizadas, resueltas e informadas a la coordinación de seguridad de la información y a las áreas responsables por su tratamiento de manera inmediata (alertas).

Se debe desarrollar un programa de tratamiento de incidentes en seguridad de la información que dé prioridad a dichas alertas y las resuelva conforme a la criticidad de la Información de NOFRAUD.

16.3 NORMAS

A. El responsable de la información debe definir los eventos considerados como críticos junto con sus respectivas alertas y registros de seguridad de la información, los cuales deberán ser generados. Estos deben ser activados, vigilados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera inmediata al equipo de reacción inmediata. Los registros y los medios que los generan

y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las pruebas.

B. Los incidentes de seguridad, resultantes del incumplimiento de la política y normas de seguridad de NOFRAUD, serán direccionados por el proceso de manejo de incidentes establecido por la coordinación de seguridad de la información, con el objetivo de realizar la respectiva investigación y entregar los resultados a los respectivos entes responsables dentro de la empresa, encargados de tomar las acciones correctivas y preventivas del caso.

C. Los empleados deberán estar informados del proceso disciplinario que se llevará a cabo en caso de incumplimiento de la política de seguridad de la información o alguno de los elementos que la soportan. En cualquier caso se hará un seguimiento de acuerdo con los procedimientos establecidos para el manejo de incidentes de seguridad.

D. Se debe crear un programa que debe incluir la definición de un equipo de reacción inmediata, con el objetivo de atender los incidentes de seguridad y otras situaciones que NOFRAUD considere como críticas para la seguridad de sus activos.

17 POLÍTICAS PARA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

17.1 PREMISAS

Los recursos de información y los procesos críticos definidos por NOFRAUD, deben contar con un plan de continuidad de negocio soportados por la empresa y estar preparados ante fallas mayores y/o desastres.

17.2 POLÍTICA

Los procesos críticos establecidos por NOFRAUD deben garantizar que sus activos de información estén disponibles para su tratamiento autorizado cuando la empresa los requiera en la ejecución de sus tareas regulares. Por lo que el responsable del proceso, debe diseñar, documentar, implementar, entrenar, divulgar y probar, mantener y medir periódicamente procedimientos para asegurar una recuperación de la operación en el tiempo requerido, sin disminuir los niveles de seguridad de la información establecidos.

17.3 NORMAS

A. Para los procesos críticos del negocio, NOFRAUD debe contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad del negocio aún en caso de desastre en las instalaciones de los lugares de operación.

B. Cada lugar debe incluir los controles establecidos para este tipo de áreas según su clasificación, para que no se vea disminuida los aspectos de seguridad en caso de desastre.

C. Se debe seguir una estrategia de recuperación alineada con los objetivos de negocio, formalmente documentada y con procedimientos perfectamente probados para asegurar la restauración de los procesos críticos del negocio, ante el evento de una contingencia.

D. Cada responsable de los procesos de NOFRAUD con el acompañamiento de la dirección de tecnología de la información, debe diseñar, implementar, probar y mantener su plan de continuidad.

E. El plan de continuidad debe considerar los siguientes aspectos:

1. Procedimientos de contingencia. Los cuales describen las acciones a tomar cuando ocurre un incidente que interrumpe las operaciones del negocio, proporcionando mecanismos alternos y temporales para continuar con el procesamiento.

2. Procedimientos de recuperación. Los cuales describen las acciones a seguir para trasladar las actividades del negocio a un centro alterno de recuperación.

3. Procedimientos de retorno. Los cuales describen las acciones a seguir para regresar las operaciones normales a las instalaciones originales.

4. Programación de pruebas. Las cuales describen la periodicidad en que el plan de continuidad debe ser probado.

5. Actualización periódica. El plan debe actualizarse cuando cambios realizados en el ambiente operativo impacten su funcionalidad.

6. Consideraciones de seguridad. Es importante que el plan sea diseñado para mantener los controles de seguridad establecidos por la empresa aun cuando se opere en modalidad de contingencia. Es responsabilidad de la coordinación de seguridad de la información asegurar que estas consideraciones sean efectivamente contempladas en el plan.

7. Cuando se realicen pruebas, simulacros o se tengan contingencias reales, los resultados y sugerencias deben ser entregadas a los responsables de la información quienes deben actualizar sus planes y mantenerlos al día conforme los riesgos de disponibilidad lo dictaminen.

8. El proceso de copia y respaldo de la información de NOFRAUD debe de contar con una política que debe cumplir con los requerimientos del negocio, los de seguridad de la información y los legales. Este proceso junto con sus procedimientos es de entrada a los planes de Continuidad de NOFRAUD.

18 CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

18.1 PREMISAS

NOFRAUD vigilará permanentemente el cumplimiento de la presente política y cuando exista una violación debe ser detectada e informada a las instancias oficiales establecidas para tal fin.

18.2 POLÍTICA

Las situaciones o acciones que violen la presente política deben ser detectadas, registradas, analizadas, resueltas y reportadas de manera inmediata a través de los canales señalados para el efecto.

Se entenderán incluidas a la política las regulaciones nacionales e internacionales que de tiempo en tiempo se expidieren y que se relacionen con la misma. Cuando de la aplicación de tales normas se presentare un conflicto, se entenderá que aplica la más restrictiva, es decir, aquella que exija el mayor grado de seguridad.

Así mismo y con el fin de mantener un nivel de seguridad en línea con el negocio de NOFRAUD, esta política se debe apoyar en las mejores prácticas de seguridad de la información y aquellos que el mercado y la empresa reconozcan como tal.

18.3 NORMAS

A. La política junto con el sistema de gestión de seguridad de la información de NOFRAUD debe ser auditado anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.

B. La información de auditoría generada por el uso de los controles de seguridad de los recursos de tecnología, debe ser evaluada por el responsable para:

   - ✓ Detectar violaciones a la política
   - ✓ Reportar incidentes de seguridad
   - ✓ Constatar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.

C. Periódicamente se debe evaluar el cumplimiento de los requerimientos de seguridad por parte de los usuarios. El incumplimiento de los requerimientos de seguridad, se debe registrar como un incidente a la política de seguridad de la información que debe ser resuelto de acuerdo con los procedimientos de Manejo de incidentes de NOFRAUD.

D. Se debe establecer en los contratos de trabajo de empleados y en los contratos de desarrollo realizados por proveedores y contratistas, cláusulas respecto a la propiedad intelectual de NOFRAUD, al material y productos generados en el desarrollo del negocio.

E. Los contratos de consultoría, y en general todo tipo de contratos de servicios deben contener provisiones a este respecto. De igual manera, dada la proliferación del "outsourcing", es especialmente importante clarificar los derechos generados por proveedores en desarrollo de este tipo de contratos.

F. Deben implementarse procedimientos apropiados para asegurar el cumplimiento con las restricciones de carácter legal en el uso de material que puede estar sujeto a derechos de propiedad intelectual tales como derechos de autor y derechos de diseño.

G. Los contratos vigentes y los futuros deben incluir dentro de sus condiciones el derecho que tiene NOFRAUD a realizar auditorías periódicas y esporádicas a las condiciones de seguridad de la información que conserven sus proveedores con el fin de garantizar la protección de la información de forma integral.