GRUPO EMPRESARIAL BOLSA MERCANTIL

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Agosto 2024

TABLA DE CONTENIDO

1. OBJETIVOS

Principal

Proteger los activos de información del GRUPO EMPRESARIAL BOLSA MERCANTIL frente a los riesgos, amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad, privacidad y confiabilidad de la información, la misión y objetivos estratégicos de la compañía; así como brindar un marco de confianza a los grupos de interés.

El objetivo principal se respalda en los siguientes objetivos específicos:

- Asegurar la implementación de controles de seguridad de la información y ciberseguridad comprendidas en esta política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
- Mantener la política general de seguridad de la información y ciberseguridad del GRUPO EMPRESARIAL BOLSA MERCANTIL actualizada, a efectos de asegurar su vigencia y nivel de efectividad.
- Definir, implementar, operar y mejorar de forma continua el sistema de gestión de seguridad de la información y ciberseguridad, soportado en directrices, estándares, normatividad vigente y aplicable.

2. ALCANCE/APLICABILIDAD

La presente política general de seguridad de la información y ciberseguridad se dicta en cumplimiento de las disposiciones legales, reglamentarios y contractuales vigentes y para atender la expectativa de las partes interesadas.

Aplica también en todo el ámbito de todo el GRUPO EMPRESARIAL BOLSA MERCANTIL, a sus activos de información, recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la compañía a través de contratos o acuerdos con terceros.

La presente política debe ser cumplida por parte de la junta directiva, la alta gerencia, todos los colaboradores de la Bolsa, incluyendo pasantes y/o practicantes, así como colaboradores contratados bajo la modalidad de outsourcing, proveedores siempre y cuando el objeto de los bienes y/o servicios afecten los activos de información, sociedades comisionistas de bolsa, participantes de los mercados y entes de control externos, independiente de cual fuere su nivel jerárquico. De igual manera se pone a disposición de las personas vinculadas a las sociedades comisionistas miembros de la Bolsa para su cumplimiento.

3. DEFINICIONES

Las definiciones de esta política se encuentran en el ANEXO 1

4. POLÍTICA

El presente documento define las políticas que tienen como objetivo para proteger a la organización de una amplia gama de amenazas, a fin de garantizar la confidencialidad, integridad, disponibilidad, legalidad, privacidad y confiabilidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del GRUPO EMPRESARIAL BOLSA MERCANTIL.

Los principios de esta política son parte de la cultura organizacional, ya que existe compromiso de la presidencia, la alta gerencia, directores, coordinadores y colaboradores para su difusión, consolidación y cumplimiento.

Esta política incluye una serie de pautas sobre aspectos específicos de la seguridad de la información, que incluyen:

- **Organización de la seguridad:** orientado a administrar la seguridad de la información dentro del GRUPO EMPRESARIAL BOLSA MERCANTIL y establece un marco gerencial para controlar su implementación.

- **Seguridad de los recursos humanos:** orientado a la adecuada aplicación de procesos de selección, contratación, desarrollo y retiro del personal.

- **Clasificación y control de activos:** Destinado a mantener una adecuada protección de los activos de información del GRUPO EMPRESARIAL BOLSA MERCANTIL

- **Control de accesos**: asegurar el oportuno acceso a los sistemas de información de acuerdo con los perfiles definidos y los privilegios asignados, así como denegar los accesos no autorizados.
- **Cifrado**: proteger la información clasificada como confidencial usando mecanismos que impidan su modificación y/o visualización por personas no autorizadas.

- **Seguridad física:** destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información del GRUPO EMPRESARIAL BOLSA MERCANTIL.

- **Gestión de las comunicaciones y la operatividad del negocio:** Dirigido a garantizar el funcionamiento correcto y seguro de los mecanismos y dispositivos de procesamiento de la información y medios de comunicación.

- **Desarrollo y mantenimiento de los sistemas:** orientado a garantizar la incorporación de medidas de seguridad de la información y ciberseguridad en los sistemas de información desde su desarrollo (seguro) y/o implementación y durante su mantenimiento.

- **Relación con proveedores**: destinado a establecer los riesgos de seguridad de la información asociados a la prestación de los servicios por parte de los proveedores de acuerdo con las directrices adoptadas por la compañía.

- **Incidentes o eventos:** orientado a adoptar procedimientos que permitan reportar incidentes o eventos de seguridad de la información a la Bolsa de manera oportuna para una efectiva gestión de estos.

- **Administración de la continuidad de las actividades:** orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres, los cuales deberán ser concordantes y coordinados con los planes de contingencia y continuidad de la GRUPO EMPRESARIAL BOLSA MERCANTIL.

- **Cumplimiento:** destinado a evitar infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos relacionados con la seguridad de información; y de los requisitos de seguridad establecidos en este documento.

La vicepresidencia de riesgos y cumplimiento al menos una vez al año o cuando se requieran revisará las políticas aquí definidas, a efectos de mantenerla actualizada frente a las necesidades de la compañía y/o requerimientos de los entes de control. Así mismo, presentará cualquier modificación que sea necesaria en función de posibles cambios que puedan afectar su definición, como cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad para la aprobación de la junta directiva. Podrá sufrir modificaciones futuras, de acuerdo con las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

Está política podrá ser revisada y/o auditada por entes independientes, como parte del proceso de mejora continua del sistema de gestión de seguridad de la información SGSI.

El presente documento se encuentra estructurado para dar cumplimiento a los requisitos regulatorios de la norma ISO/IEC 27001:2013, como un marco de referencia para la gestión de la seguridad de la información en la compañía.

4.1 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como la preservación de la:

- **Confidencialidad:** propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. Es decir, hace referencia a la protección de información cuya divulgación no está autorizada.

- **Integridad:** la información precisa, coherente y completa desde su creación hasta su destrucción.

- **Disponibilidad:** la información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Adicionalmente, son considerados los siguientes conceptos:

- **Legalidad:** para garantizar el cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta el GRUPO EMPRESARIAL BOLSA MERCANTIL en materia de seguridad de la información y ciberseguridad.

- **Confiabilidad de la Información:** la información debe ser la apropiada para la administración de la compañía y el cumplimiento de sus obligaciones.

- **Autenticidad:** para asegurar la validez de la información en tiempo, forma y distribución. Asimismo, garantizar el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Auditabilidad:** los eventos significativos de los sistemas de información son registrados para su control posterior (logs de los diferentes ambientes de producción).

- **Protección a la duplicación:** para impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original. Por lo anterior, una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

- **No repudio:** Para evitar que una compañía que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

4.2 RESPONSABILIDADES Y PRINCIPIOS ORIENTADORES

Estas políticas son de aplicación a todos los grupos de interés del GRUPO EMPRESARIAL BOLSA MERCANTIL, cualquiera sea su situación, en el proceso al cual se encuentre vinculado y cualquiera sea el nivel de las tareas que desempeñe; por tanto, estos deberán desplegar sus mejores esfuerzos para asegurar que su conducta se ajuste a los más altos niveles de disciplina, profesionalismo y seriedad en aras de preservar el buen funcionamiento de los sistemas y la información, su integridad, confidencialidad, y disponibilidad, así como la confiabilidad del público mismo.

Se consideran violaciones graves el robo, daño, divulgación, secuestro de información reservada o confidencial.

Los miembros de la junta directiva en el ejercicio de su cargo deben aplicar la presente política y en especial preservarán la confidencialidad sobre aquella información que así lo requiera. Así mismo, aplicarán las medidas de seguridad respecto de los sistemas de información a los cuales se les de acceso para el desarrollo de sus funciones.

Si bien todos los colaboradores deben cumplir esta política, la presidencia, los vicepresidentes, , directores y coordinadores son responsables de la aplicación de esta política dentro de sus procesos

de responsabilidad, así como velar por el cumplimiento de dicha política por parte de su equipo de trabajo.

La vicepresidencia de riesgos y cumplimiento:

- Revisa y propone a la junta directiva las políticas de seguridad de la información y ciberseguridad, y las funciones generales en materia de seguridad de la información para su aprobación.

- Monitorea cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

- Toma conocimiento y supervisa la investigación y monitoreo de los incidentes relativos a la seguridad de la información y ciberseguridad.

- Da trámite para obtener la aprobación de las iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada proceso, así como acuerda y aprueba metodologías y procesos específicos relativos a seguridad de la información y ciberseguridad.

- Garantiza que la seguridad sea parte del ciclo de vida de la información.

- Evalúa y coordina la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios. Promueve la difusión y apoyo a la seguridad de la información y ciberseguridad dentro del GRUPO EMPRESARIAL BOLSA MERCANTIL.

La vicepresidencia de talento humano y gestión administrativa será la responsable de la seguridad física e instalaciones.

Adicionalmente, la alta gerencia, o a quien designe la misma, debe coordinar el proceso de administración de la continuidad de las actividades de la organización.

Los propietarios de la información son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de esta, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios tienen permisos de acceso a la información de acuerdo con sus funciones y competencia.

El responsable de formación y entrenamiento debe velar porque todo el nuevo personal de la Bolsa, incluyendo los usuarios terceros, conozca sus obligaciones respecto del cumplimiento de las políticas de seguridad de la información y ciberseguridad y de todas las normas, procedimientos y prácticas que de ella surjan.

Así mismo, tiene a su cargo la notificación de la presente política a todo el personal con el apoyo de la vicepresidencia de riesgos y cumplimiento; de los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de confidencialidad, cláusulas adicionales en los contratos laborales que sean requeridas, acuerdos u otra documentación del GRUPO

EMPRESARIAL BOLSA MERCANTIL con sus colaboradores y las tareas de capacitación periódica en materia de seguridad.

La vicepresidencia de tecnología tiene a su cargo la función de cubrir los requerimientos de seguridad informática y ciberseguridad establecidos para la operación que sean definidos en las políticas de seguridad de la información y por parte de la vicepresidencia de riesgos y cumplimiento, así como la administración y comunicación de los sistemas y recursos de tecnología del GRUPO EMPRESARIAL BOLSA MERCANTIL.

La vicepresidencia jurídica y secretaría general debe verificar la inclusión de cláusulas de cumplimiento de la presente política y otras que en esta materia sean aplicables en la gestión de todos los contratos con terceros no laborales. Asimismo, asesora en materia legal al GRUPO EMPRESARIAL BOLSA MERCANTIL, en lo que se refiere a la seguridad de la información.

Los usuarios que realicen tratamiento de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información y ciberseguridad vigente.

La auditoría interna es responsable de practicar auditorías periódicas al sistema de gestión de seguridad de la información SGSI, sobre los activos de información, sistemas de información y actividades vinculadas con la tecnología de información, y de informar sobre el cumplimiento de los controles establecidos en la presente Política.

La junta directiva del GRUPO EMPRESARIAL BOLSA MERCANTIL puede proponer modificaciones y actualizaciones a los términos de la presente política en cualquier momento. El usuario tiene la responsabilidad de revisar periódicamente la versión más actualizada de estos términos a través del enlace proporcionado para la publicación de estos en la herramienta que para este fin disponga el GRUPO EMPRESARIAL BOLSA MERCANTIL.

4.3 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La Bolsa cuenta con un sistema de gestión de seguridad de la información - SGSI que tiene alcance a todos los productos, proyectos y procesos de la Bolsa toda vez que estos tienen implícitos el uso de activos de información que deben ser protegidos en función del nivel requerido de confidencialidad, integridad y disponibilidad.

Este sistema cuenta con una política general mencionada anteriormente y las siguientes cada una con sus respectivos objetivos, alcance, responsables entre otros aspectos que de igual manera a la principal son de obligatorio cumplimiento:

- **POLÍTICA INTERNA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS:**

Establece las directrices para la adquisición, desarrollo y mantenimiento de los sistemas de información de la organización, garantizando la seguridad de dichos sistemas.

Ver anexo No. 2.

- **POLÍTICA INTERNA DE CONTROL DE ACCESO:**

Establece las directrices para:

  - Prevenir el acceso no autorizado a los sistemas de información.
  - Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
  - Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
  - Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.
  - Restringir el acceso a los programas y archivos y establecer los niveles de acceso.
  - Asegurar que los datos, archivos y programas sean utilizados correctamente.

Ver anexo No 3.

- **POLÍTICA INTERNA DE CONTROLES CRIPTOGRÁFICOS**

Establecer las directrices necesarias para proteger la confidencialidad, integridad, disponibilidad y autenticidad de los activos de información del Grupo empresarial bolsa mercantil.
Ver anexo No. 4

- **POLÍTICA INTERNA DE DISPOSITIVOS MÓVILES**

Establecer las condiciones para el manejo de los dispositivos móviles que acceden a información del Grupo Empresarial Bolsa Mercantil, a fin de garantizar y velar por el uso responsable de estos por parte del personal.
Ver anexo No. 5

- **POLÍTICA INTERNA DE ACTIVOS DE INFORMACIÓN**

Dar a conocer las directrices para que los activos de información reciban un adecuado manejo y protección.
Ver anexo No. 6.

- **POLÍTICA INTERNA DE LAS OPERACIONES Y COMUNICACIONES**

Establecer las directrices para garantizar la documentación, mantenimiento y actualización de los procedimientos de operación y administración de la plataforma tecnológica.
Ver anexo No 7.

- **POLÍTICA DE RELACIÓN CON TERCEROS**

Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas. Ver anexo No. 8.

- **POLÍTICA INTERNA DE SEGURIDAD DEL RECURSO HUMANO**

Establece la directriz general que cumple el proceso de talento humano para la selección, capacitación, permanencia y desvinculación de los colaboradores de la organización.
Ver anexo No. 9

- **POLÍTICA INTERNA DE SEGURIDAD FÍSICA Y DEL ENTORNO**

Definir las directrices para prevenir el acceso no autorizado a las instalaciones de la Bolsa y áreas de acceso Restringido, evitar la pérdida y/o daño de los activos de información y la interrupción del negocio.
Ver anexo No. 10

- **POLÍTICA INTERNA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGUIRDAD**

Establecer las directrices para facilitar la respuesta y/o recuperación rápida ante eventos y/o incidentes de seguridad de la información y/o ciberseguridad minimizando la pérdida de confidencialidad, integridad o disponibilidad de la información o la interrupción de servicios del Grupo empresarial bolsa mercantil.
Ver anexo No. 11

- **POLÍTICA INTERNA DE MONITOREO DE ALERTAS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD**

Establecer las directrices para las actividades de monitoreo de alertas de las herramientas y servicios de Ciberseguridad que tengan implementada en el Grupo empresarial , para la detección y prevención de Ciberataques que lleguen a afectar la Confidencialidad, Integridad y Disponibilidad de la Información corporativa y de sus clientes.
Ver anexo No. 12

- **POLÍTICA INTERNA ESCRITORIO Y PANTALLA LIMPIA**

La organización establece las directrices de escritorio y pantalla limpios con el propósito de reducir los riesgos de perdida, modificación y acceso no controlado de la información, durante y fuera de las actividades laborales.
Ver anexo No. 13

En relación con estas políticas se ha establecido un plan de monitoreo del cumplimiento de estas y derivado de los resultados de este ejercicio se establecen las oportunidades de mejora en cuanto al fortalecimiento de las medidas de mitigación del riesgo.

Para el correcto funcionamiento del SGSI, la organización aplica una metodología de gestión de los riesgos de seguridad de la información y ciberseguridad para identificar, medir, controlar y

monitorear los riesgos asociados a los activos de información de tal manera que se pueda asegurar la confidencialidad, integridad y disponibilidad de estos.

Para la adecuada articulación del SGSI se cuenta con:

- Una matriz RACI que establece las responsabilidades y segregación de funciones frente al sistema por parte de las distintas áreas y cargos relacionados con este.

- Una matriz de activos de información que contiene los activos de información y su evaluación de impacto en términos de confidencialidad, integridad y disponibilidad.

- Una matriz de control de acceso en la que se lleva el control de acceso por cargo y perfil de los colaboradores a los diferentes sistemas y servicios de información.

- Una matriz de riesgos, donde se gestionan los riesgos de los procesos de la cadena de valor de la Bolsa en términos confidencialidad, integridad y disponibilidad, así como la definición de los controles relacionado con el Anexo A de la ISO 27001:2013 y planes de tratamiento de riesgos.

- Gestión de vulnerabilidades – Hardening – Ethical Hacking mediante la cual se realiza el escaneo de vulnerabilidades a todos los sitios web expuestos a internet e internos Core del Negocio, sistema operativo de las instancias y servidores, certificados digitales, cumplimiento de línea base de seguridad Hardening, ejercicios de Ethical Hacking y vectores de ataques. Todo lo anterior para validar la exposición, impacto y prevención de ciberataques externos y/o internos.

- Un monitoreo de alertas de Ciberseguridad SOC que se tiene tercerizado, para el servicio de monitoreo de SOC 7x24, contemplando alertas, detección temprana de ciberataques, así como la ejecución de acciones predefinidas o Playbooks (libro de jugadas) en caso de ataques de Ransomware, elevación de privilegios, denegación de servicios, entre otros.

- Monitoreos internos de seguridad de la información y ciberseguridad:
    - Control de instalación de software
    - Alertas antivirus y maliciosas
    - Conexiones remotas
    - Usuarios y perfiles de acceso
    - Actividades de los usuarios administradores
    - Alertas de correo maliciosos o phishing
    - Control de navegación
    - Control de fuga de información
    - Política de contraseñas
    - Actividades de usuarios

- Gestión de seguridad de la información en proyectos y terceros: todo proyecto que tenga la compañía pasa por validaciones de seguridad de la información y ciberseguridad; se evalúa la adquisición de software, servicios o contratación de terceros que vayan a tratar

información de clientes o de la compañía. Adicionalmente se lleva control y seguimiento a los proveedores críticos.

- Se cuenta con programas de capacitación y sensibilización hacia todos los colaboradores.

- Respecto de la gestión del sistema y de los riesgos de seguridad de la información se presentan informes a la junta directiva y el comité de riesgos para obtener su retroalimentación en aras de la mejora continua.

- Adicionalmente, la alta gerencia por medio de las auditorías internas y revisoría fiscal, valida el cumplimiento de las políticas y directrices de seguridad de la información de la compañía. El resultado de estas, se presentan al comité de auditoría para hacer seguimiento de los planes de acción acordados.

4.4 NIVEL DE CUMPLIMIENTO

El incumplimiento de esta política traerá consigo consecuencias administrativas, disciplinarias, penales y/o las legales que apliquen de acuerdo con la normativa interna vigente e incluyendo aquellas que competen al gobierno nacional en cuanto a seguridad, privacidad de la información, ciberseguridad y gobierno digital que sea referido.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cabal cumplimiento a la presente política.

El GRUPO EMPRESARIAL ha decidido definir, implementar, operar y mejorar de forma continua un modelo de seguridad, ciberseguridad y privacidad de la información, soportado en lineamientos claros enfocados a las necesidades de sus partes interesadas.

Las políticas que soportan el modelo de seguridad de la información y ciberseguridad del Grupo empresarial bolsa mercantil, deben ser revisados por la vicepresidencia de riesgos y cumplimiento aprobadas por la junta directiva o instancia que esta designe mínimo anualmente, a través de los cuales el GRUPO EMPRESARIAL BOLSA MERCANTIL asegura que:

- Las responsabilidades frente al modelo de seguridad, ciberseguridad y privacidad de la información sean definidas, compartidas, publicadas y aceptadas por los grupos de interés que tenga relación contractual, jurídica, traten información o servicios del GRUPO EMPRESARIAL BOLSA MERCANTIL.
- Se proteja la información creada, procesada, transmitida y/o resguardada por los procesos que intervienen para alcanzar los objetivos estratégicos definidos por el GRUPO EMPRESARIAL BOLSA MERCANTIL, y en el cumplimiento de las funciones de la organización, con el fin de minimizar impactos financieros, operativos y/o legales debido a un uso incorrecto de ésta. Para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad y/o custodia.
- Se proteja su información frente a amenazas originadas por parte del personal custodio, responsable y/o usuarios de esta.

- Se proteja los centros de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Se controle la operación de sus procesos misionales, garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Se implemente mecanismos de control de acceso a la información, sistemas y recursos de red.
- Se garantice que la seguridad, ciberseguridad y privacidad de la Información sean parte integral del ciclo de vida de los sistemas de información.
- Se garantice, a través de una adecuada gestión de los eventos, la atención de los incidentes de seguridad, ciberseguridad y privacidad de la Información y las vulnerabilidades identificadas y asociadas con los sistemas de información proporcionando una mejora efectiva de su modelo de seguridad.
- Se garantice la continuidad de los procesos críticos de la organización ante eventos que puedan afectar su operación.
- Se garantice el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

- Se garantice el uso, acceso y custodia de la información, clasificada como reservada, en cumplimiento de las disposiciones establecidas en la CE008 de la SFC.

Todo el personal del GRUPO EMPRESARIAL BOLSA MERCANTIL, incluyendo los grupos de interés con acceso a los sistemas de información y/o información de la organización, serán responsables de protegerla de acuerdo a los niveles de acceso, manejo, transferencia y/o destrucción, para garantizar esto, deberán conocer la política general de seguridad, ciberseguridad y privacidad de la información, así como sus lineamientos internos y demás documentos que apoyen el desarrollo de la misma al interior de la organización, estando en la obligación de manifestar comportamientos incorrectos a nivel de seguridad, ciberseguridad y/o privacidad como parte de su trabajo diario.

La política general de seguridad de la información y ciberseguridad se encuentra regida por los lineamientos de obligatorio cumplimiento definidos por la Superintendencia Financiera de Colombia - SFC, el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y demás organizaciones de control, acorde a lo incorporado en el documento CONPES 3701 de 2011 y 3854 de 2016 para la implementación de dicha política.

4.5 ESTRUCTURA DE GOBIERNO

Junta directiva: aprobar la política de seguridad, ciberseguridad y privacidad de la información y hacer seguimiento, pronunciándose sobre la gestión del modelo definido para el cumplimiento de esta y tomar las decisiones que considere pertinentes frente a seguridad de la información, a partir de los reportes que contengan los resultados de la gestión que se generen de las revisiones anuales, semestrales o cuando se requiera por cambios normativos o cuando la situación lo amerite.

Presidencia (CEO- Chief Executive Officer): su función principal será la de supervisar y velar porque la estrategia definida para el desarrollo, implementación, gestión y seguimiento del modelo de seguridad, ciberseguridad y privacidad de la información en la organización cumpla con la consecución de los objetivos de esta, además de definir revisar y aprobar, directamente o a través

de la instancia que esta designe, los principios a seguir dentro de la organización en el marco de la presente política.

Vicepresidencia de Riesgos y Cumplimiento (CISO – Chief Information Security Officer): el rol es ejecutado por el gerente corporativo de riesgos y su función principal es ser el responsable en el monitoreo y verificación del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información y ciberseguridad, sin perjuicio a aquellas tareas que realiza la auditoría interna[1] y es el responsable del programa de tratamiento de datos personales en la Organización.

Oficial de seguridad (CSO - Chief Security Officer): este rol es ejecutado por un profesional senior de la dirección de riesgos o quien designe el CISO y su función principal es identificar qué activos de información necesitan protección y cómo deben protegerse emitiendo lineamientos y estrategias, así como liderar la implementación de esas medidas de protección en conjunto con los responsables de los controles.

Vicepresidencia de tecnología se encarga de que las estrategias de la organización estén alineadas con la tecnología de la información para lograr los objetivos planificados, de mejorar los procesos de tecnologías de la información de la organización, gestionar los riesgos de TI y la continuidad de negocio en el componente del DRP, controlar el coste en infraestructura de tecnologías de la información, alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, establecer mejoras e innovaciones de soluciones y productos y gestiona del día a día de las tecnologías de la información.

Vicepresidencia financiera (CFO – Chief Financial Officer) – Interacción con CTO: su función es garantizar que el sistema de seguridad de la información y ciberseguridad se le asignen los recursos necesarios para la adecuada ejecución del sistema y sus controles.

Vicepresidencia de talento humano y gestión administrativa: su rol es el de implementar los controles definidos que garanticen la seguridad de la información necesaria antes de la contratación, durante la ejecución del empleo y después de terminar el empleo o cambiar de rol dentro de la organización, así mismo garantizar la seguridad física es la de proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministros. Finalmente, de la coordinación y administración de los programas de formación y capacitación de los colaboradores

Vicepresidencia jurídica y secretaría general (CLO – Chief Legal Officer): este rol es ejecutado por el vicepresidente jurídico y secretario general. Su función es Identificar los requisitos legales, estatutarios, reglamentarios y contractuales (no laborales) pertinentes a seguridad, ciberseguridad y privacidad de la información.

Auditoría interna – Informar al CEO: Su función principal es planificar, establecer, implementar y mantener uno o varios programas de auditoría de seguridad, ciberseguridad y privacidad de la información que incluyan la frecuencia, métodos, responsabilidades, requisitos de planificación y

[1] Numeral 3.2.6 Circular Externa 007 de 2018 expedida por la SFC.

elaboración de informes, asegurando la objetividad e imparcialidad en los procesos de auditoría e informar los resultados de estas a las instancias que corresponda.

4.6 USO ACCESO Y CUSTODIA LA TOMA DE POSESIÓN

La vicepresidencia de riesgos y cumplimiento en coordinación con la vicepresidencia jurídica y secretaría general y demás que se considere, establecerán el protocolo para garantizar el acceso a la información y a la administración de los sistemas de información que operan en la nube a la SFC, Fogafín, Fogacoop, o quienes éstas designen, en el evento de toma de posesión de las entidades que conforman el grupo empresarial.

5. HISTORIAL DE CAMBIOS DEL DOCUMENTO

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
0	21/11/2018	Versión Inicial Aprobada por la Junta Directiva en sesión 597 del 28 de noviembre de 2018.
1	16/07/2019	Modificación numeral 4 – Documento Aprobado por la Junta Directiva en sesión 607 del 26 de junio de 2019.
2	20/01/2022	• Revisión y actualización integral a la política con el apoyo de los consultores de Innovinc SAS. • Actualización de cargos de acuerdo con la nueva estructura organizacional. Aprobado en sesión ordinaria de la Junta Directiva No. 652 del 20 de enero de 2022. Presentado y aprobado en Comité de Calidad en sesión del 31 de enero de 2022.
3	28/07/2023	Aprobado en sesión ordinaria de la Junta Directiva No. 677 del 19 de julio de 2023. • Ajustes en el objetivo de la política, nombre de la política (se quita privacidad por existencia de la política de protección y privacidad de datos), inclusión de nuevos monitoreos de seguridad y controles. • Ajustes de redacción de palabras con mayúsculas. • Cambio nombre de la Bolsa por grupo empresarial para que tenga alcance a las compañías de la . Presentado y aprobado en Comité de Calidad en sesión del 28 de julio de 2023.

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
4	16/08/2024	• Se realizan ajustes generales por cambio de estructura organizacional. • Se crea el anexo No. 1 correspondiente a definiciones • Se ajusta el numeral 4.3 sistema de gestión de seguridad de la información, al convertir la mención de las directrices y políticas de seguridad de la información. • Se incluyen menciones en el numeral 4.3 y se agrega el numeral 7 para dar cumplimiento a requerimientos normativos. • Se crean tres nuevas políticas: o Política de Gestión de Incidentes de seguridad de la información y Ciberseguridad o Política de Monitoreo de alertas de Seguridad de la Información y Ciberseguridad o Política de pantalla y escritorio limpio • Se agregan como anexos a este documento las políticas anteriormente llamadas directrices. Aprobado en sesión ordinaria de la Junta Directiva No. 693 del 15 de agosto de 2024 Presentado y aprobado en comité de calidad en sesión del 16 de agosto de 2024

ANEXOS

ANEXO No. 1 – DEFINICIONES

ADMINISTRADOR DE LA APLICACIÓN O DEL SISTEMA

El responsable de asignar las funcionalidades de cada uno de los accesos o derogación de permisos a los módulos u opciones del sistema acordes a la funcionalidad operativa de cada uno de los usuarios en la aplicación o sistema.

ACCESO

Actividad de permitir, entrar y/o interactuar a un lugar o sistema de información.

ACCESO REMOTO

Conexión de 2 dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación ya sean telefónicas o por medio de redes de área ampliada que permiten el acceso de aplicaciones e información de la red.

ADMINISTRACIÓN DE RIESGOS

Se entiende por administración de riesgos el proceso de identificación, medición, control y mitigación, a un costo aceptable, de los riesgos de seguridad que pueden afectar a la información. Dicho proceso es cíclico y es llevado a cabo en forma periódica mediante la actividad de monitoreo.

AGENTE DE ANTIMALWARE

Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos o maliciosos en sistemas informáticos.

ALERTA DE CIBERSEGURIDAD: son notificaciones o avisos de posibles peligros que puede estar expuesta una compañía por la posible actividad de un ciberataque a los usuarios o sistemas de información.

AUTENTICACIÓN

Es la propiedad que permite identificar el generador de la información. Por ejemplo, al recibir un mensaje de alguien, estar seguro de que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.
Esta propiedad se puede considerar como un aspecto de la integridad si está firmado por alguien, está realmente enviado por el mismo.

AUTORIZACIÓN

Proceso de asignar a los usuarios permisos para realizar actividades de acuerdo con su perfil o función dentro del grupo empresarial.

ATAQUE CIBERNÉTICO

Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de esta o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

BLUE TEAM

Hace referencia al equipo que se encarga de detener o responder a los ataques simulados por parte del Red team.

BOTNET

Es una red de equipos que han sido infectados con software malicioso, para permitir su control remoto, obligándoles a propagar malware, enviar spam o realizar ataques de denegación de servicio distribuido (DDoS), sin el conocimiento o el consentimiento de los propietarios de los equipos.

CAMBIO

Adición, modificación o eliminación de un servicio o componente autorizado, planificado o de soporte y su documentación relacionada.

CCOC

Comando Conjunto Cibernético de Colombia que planea, coordina, integra y conduce operaciones militares en el ciberespacio para la defensa de los intereses nacionales y de la infraestructura crítica cibernética.

CIBERATAQUE: es un intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar un activo. Un ciberataque o ataque informático, es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático.

CIBERSEGURIDAD

Controles para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la organización.

CLIENTE

Equipo informático cuyo papel habitual es el de consumir servicios ofertados por otros equipos informáticos. Es el caso de los ordenadores personales situados en los puestos de trabajo.

CÓDIGO MÓVIL

Código que se descarga y ejecuta en el equipo con poca o ninguna intervención del usuario. Entrarían en esta categoría, p. ej., todo tipo de scripts (Java, VB...), macros, controles Active X, applets (Java, Flash...), etc.

CONTROL DE ACCESO

Mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo de información.

CORREO ELECTRÓNICO

Servicio de red que permite a los clientes enviar y recibir mensajes electrónicos de textos, imágenes, videos, audio, u otros contenidos, mediante sistemas de comunicación electrónicos.

CUENTAS DE USUARIO

Identificador asignado a un usuario del sistema para el acceso y uso de la computadora, sistemas, aplicaciones, red, etc.

CUENTAS DE GRUPO

Su uso es para servicios de email, donde varios usuarios de un mismo equipo comparten una cuenta de correo electrónico para gestión del proceso.

CUENTA DE SERVICIO

Se usan para ejecutar algún proceso, tarea, o trabajo dentro de un sistema de información. La administración de estas cuentas de servicios está a cargo de la Vicepresidencia de Tecnología.

CIFRAR

Es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) que transforma la información, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta.

CIFRADO

Es un mecanismo específico para poder convertir la información en un código diferente que pueda ser descifrado sólo por las personas autorizadas.

CIBERSEGURIDAD

Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

CIBERAMENAZA

Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

CIBERESPACIO
Corresponde a un ambiente complejo resultante de la interacción de personas, software y servicios en Internet, soportado en dispositivos tecnológicos y redes conectadas a la red mundial, propiedad de múltiples dueños con diferentes requisitos operativos y regulatorios.

COLCERT

Grupo de Respuesta a Emergencias Cibernéticas de Colombia, tiene como responsabilidad la coordinación de la Ciberseguridad y Ciberdefensa Nacional.

CONTROL DE ACCESO

Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.

CRYPTO MINER

Software malicioso diseñado para la ejecución de transacciones con criptomonedas realizando uso del procesamiento de los equipos infectados.

CRYPTOJACKING

Uso no autorizado de dispositivos, aplicaciones o sitios web para ejecutar minería de criptomonedas.

DATOS PERSONALES

Información que contiene elementos que al unirse pueden caracterizar a un individuo, por ejemplo, número de cédula, dirección, tipo de sangre, teléfono, etc.

DISPOSITIVO MÓVIL

Elemento electrónico con capacidad de procesamiento de datos, conexión a Internet y memoria con fácil capacidad de ser trasportados por el usuario final. Son ejemplos de estos: celulares inteligentes, tabletas, agendas digitales, relojes inteligentes, cámaras digitales, discos duros, USB y portátiles.

EJECUTORE DEL CONTROL DE ACCESOS

Asignar los roles y perfiles a los usuarios solicitantes (creación, des habilitación, reasignación)

EVALUACIÓN DE RIESGOS

Se entiende por evaluación de riesgos el análisis de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de esta, para determinar la probabilidad de que ocurran y su potencial impacto en la operación del Grupo empresarial bolsa mercantil.

EVENTO DE CIBERSEGURIDAD
Ocurrencia de una situación que **podría** afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

FALSA ALARMA

Evento o situación que después de un análisis inicial, se descarta como incidente.

FUNCIONES

Son el conjunto de responsabilidades, tareas, actividades necesarias a desempeñar.

GESTIÓN DE CAMBIO

Evaluación y planificación del proceso de cambio para asegurar que se realice de la forma más eficiente, siguiendo los procedimientos establecidos y asegurando en todo momento la calidad y continuidad de los servicios de TI.

INFORMACIÓN SENSIBLE

Se refiere a toda la información confidencial o restringida. La información sensible es toda aquella información importante para el negocio, que debe ser vigilada, controlada y no es de conocimiento púbico.

IDENTIFICACIÓN Y AUTENTICACIÓN

Corresponde al registro de un usuario en un sistema de información que permite identificarlo plenamente mediante el nombre de usuario y clave.

IDS

El sistema de detección de intrusos aporta a la red un grado de seguridad de tipo preventivo ante de cualquier actividad sospechosa. El sistema IDS consigue este objetivo a través de alertas anticipadas dirigidas a los administradores de sistemas.

INCIDENTE DE SEGURIDAD O CIBERSEGURIDAD

Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

INCIDENTE SIGNIFICATIVO

Son incidentes que afectan los activos de información, procesos, servicios o el sistema de gestión con consecuencias que comprometen la imagen, reputación, o terminan en pérdidas económicas para la organización durante tiempos prolongados.

INCIDENTE MENOR

Son incidentes que no comprometen la operación normal de los activos de información, procesos, servicios o el sistema de gestión, es decir, que pueden ser controlados en forma paralela a la operación.

INFORMÁTICA FORENSE

Aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información.

INFORMACIÓN

Toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

INFORMACIÓN EN REPOSO

Datos guardados en dispositivos de almacenamiento persistente (por ejemplo, recursos AWS, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).

INFORMACIÓN EN TRANSITO

Información que fluye a través de la red pública, como Internet, y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial.

INSTANCIA EN NUBE

Es un servidor virtual en la nube, donde se instala y configura el sistema operativo, aplicaciones u otros servicios tecnológicos.

IMPACTO

Magnitud del daño ocasionado a un activo en caso de que se materialice una amenaza.

IPS

El sistema de prevención de intrusos es un dispositivo que ejerce el control de acceso en una red para proteger a los sistemas de ataques. Está diseñado para analizar los datos del ataque y actuar en consecuencia, deteniéndolo en el mismo momento en que se está gestando.

LLAVES CRIPTOGRÁFRICAS

Son códigos (algoritmos) que se generan de forma automática y se guardan en un directorio especial durante la instalación. Habitualmente, esta información es una secuencia de números o letras mediante, la cual, en la criptografía se especifica la transformación del texto plano en texto cifrado o viceversa.

MECANISMO

Se consideran mecanismo los firewalls, hardware de redes y telecomunicaciones, servidores, servicios de TI (VPN, AWS, Office 365), etc.

NECESIDAD DE CONOCER (NEED-TO-KNOW)

Principio de mínimo conocimiento, también conocido como «need-to-know». Principio que al aplicarlo deberá garantizar que cada persona de la organización accederá únicamente a lo que necesita saber para la ejecución de sus funciones, ni más ni menos.

MATRIZ RACI

Matriz que define las responsabilidades de cada role en materia de seguridad de la información considerando la estructura y procesos de la organización.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Es el cargo de Profesional Senior de Seguridad de la Información de la Vicepresidencia de Riesgos.

PERSONAL

Es aquella persona que tiene una relación con el grupo empresarial, directa o a través de un tercero, bajo cualquier tipo de vinculación: planta, contratistas, proveedores, estudiantes en práctica, etc.

PERFIL
Es la descripción clara del conjunto de capacidades y competencias que identifican la formación de una persona para encarar responsablemente las funciones y tareas de una determinada profesión o trabajo.

RECURSO INFORMÁTICO

Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos en nube (cloud) u Onpremise.

RED TEAM

Simulación de ataques, asumiendo el rol de atacante y empleando las mismas técnicas, tácticas y procedimientos.

RESPONSABLE DE LA INFORMACIÓN
Funcionario de la Bolsa que es el encargado de mantener y/o gestionar el activo de información.

RESPONSABLE DE LA POLÍTICA

Es la persona que cumple la función de supervisar el cumplimiento de la presente política y de asesorar en materia de seguridad de la información a los integrantes del GRUPO EMPRESARIAL BOLSA MERCANTIL que así lo requieran.

SISTEMA DE INFORMACIÓN

Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

SISTEMA MISIONAL

Corresponde a los sistemas que soportan la operación CORE del negocio en el GRUPO EMPRESARIAL BOLSA MERCANTIL.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la organización.

RIESGO CIBERNÉTICO

Posibles resultados negativos asociados a los ataques cibernéticos.

ROL

Se refiere al conjunto de tareas y/o actividades que debe cumplir una persona que ocupa un cargo laboral

SISTEMA DE COMANDO DE INCIDENTES (SCI)

Es la combinación de instalaciones, equipamiento, personal, procedimientos, protocolos y comunicaciones, operando en una estructura organizacional común, con la responsabilidad de administrar los recursos asignados para lograr efectivamente los objetivos pertinentes a un evento, incidente u operativo. Todo lo relativo a este sistema se encuentra documentado y publicado en el "Manual de Lineamientos del Sistema de Comando de Incidentes".

SISTEMA DE INFORMACIÓN

Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

TECNOLOGÍA DE LA INFORMACIÓN

Se refiere al hardware y software operados por la Bolsa Mercantil o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Grupo Empresarial Bolsa Mercantil, sin tener en cuenta la tecnología utilizada.

TERCERAS PARTES

Son los proveedores, contratistas, entidades de control o clientes que puede tener relación con el grupo empresarial.

TEXTO PLANO

Archivo informático que contiene únicamente texto formado por caracteres que son legibles por humanos, careciendo de cualquier tipo de formato tipográfico. También son llamados archivos de texto simple o sin formato.

TRIAGE

Evaluación inicial de un evento de seguridad, a través del cual se determina si es una falsa alarma o es un incidente real.

USUARIO

Término utilizado para distinguir a cualquier persona que utiliza algún sistema, computador o aplicación o infraestructura del Grupo Empresarial Bolsa Mercantil.

USUARIO INFORMACIÓN

Se refiere tanto usuario interno (colaborador), como usuario externo (Firmas comisionistas, organismos de control, proveedores), que haga uso de la información del Grupo Empresarial Bolsa Mercantil.

USUARIOS TERCEROS

Personal temporal, personal de órganos de control): todas aquellas personas naturales o jurídicas, que no son colaboradores del Grupo Empresarial Bolsa Mercantil, pero que por las actividades que realizan en la compañía, deban tener acceso a recursos informáticos.

VISITANTE O PERSONA EXTERNA

Persona que no pertenece al grupo empresarial. Entre los cuales tenemos: proveedores, clientes, comisionistas, autoridades y otros.

VULNERABILIDAD

Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.

WHALING

Método que usan los cibercriminales para simular correos provenientes de cargos de nivel superior en una organización y así con el objeto de solicitar transferencias de dinero, conseguir información confidencial u obtener acceso a los sistemas de información.

ZONA DE SEGURIDAD

Conjunto de nodos de una red que comparten finalidad, condiciones de conectividad, medidas de seguridad y modelo de asignación de ancho de banda.

ANEXO No. 2 – POLÍTICA INTERNA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

ALCANCE/APLICABILIDAD

Aplican al personal y/o tercero de las diferentes áreas del grupo empresarial que realicen actividades de adquisición, desarrollo y mantenimiento de los sistemas de información de la organización.

La información contenida en el presente documento es de aplicación exclusiva para el grupo empresarial o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

RESPONSABILIDADES

Es responsabilidad del líder del desarrollo del proyecto, cumplir y hacer cumplimiento de la presente política, así mismo exigir el cumplimiento a los proveedores que hacen desarrollo a la vicepresidencia de tecnología garantizará las condiciones para la ejecución de la presente política.

DIRECTRIZ INTERNA GENERAL

1. REQUISITOS DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones del negocio, servicios, aplicaciones bajo el modelo por servicios (SAAS) y aplicaciones desarrolladas para usuarios. Todos estos sistemas de información son evaluados antes de su implementación o desarrollo para definir y verificar el cumplimiento de los requerimientos funcionales, de seguridad y control que tenga el sistema.

Se establecen controles para proteger la información que es considerada sensible de acuerdo con la clasificación resultante del activo de información y de esta forma evitar la posibilidad de una acción de repudio por parte de un usuario del sistema. Se aseguran los archivos del sistema y se mantiene un control adecuado de los cambios que puedan presentarse.

2. ANÁLISIS Y ESPECIFICACIONES DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

Durante la adquisición de las aplicaciones, se identifican, documentan y aprueban los requerimientos de seguridad a incorporar durante la etapa de implementación. Adicionalmente, se diseñan controles de validación de datos de entrada, procesamiento interno y salida de datos.

El grupo empresarial asegura que se realiza el análisis e implementación de los requerimientos de seguridad en el software y/o sistemas de información que se adquieran o se desarrollen previo a la puesta en producción, lo cual incluye controles de autenticación y auditoría de usuarios, verificación de los datos de entrada y salida, y la implementación de buenas prácticas para un desarrollo seguro. En algunos casos el componente de seguridad se podrá validar en producción siempre y cuando haya surtido el procedimiento de gestión de cambios que lo autorice.

El grupo empresarial cuenta con un inventario actualizado del software de su propiedad, el comprado a terceros, el adquirido bajo licenciamiento, el utilizado por subscripción, el entregado y el recibido en comodato.

Las licencias de software se almacenan bajo los adecuados niveles de seguridad y se registran en el inventario; en este se referencia el número de usuarios permitidos por licencia y la fecha de cuando se debe renovar.

El control y administración del software del grupo empresarial es responsabilidad de la vicepresidencia de tecnología, al igual que la aprobación para la adquisición o actualización de software del grupo empresarial.

Los contratos con proveedores incluyen temas sobre los requisitos de la seguridad de la información relativas a confidencialidad, destrucción controlada de información, continuidad del negocio, auditoría, entre otras de acuerdo con el objeto del contrato.

Todo software antes de ser puesto en producción se implementa y ensaya en ambientes de pruebas similares al de producción, para verificar su funcionalidad y requisitos de seguridad.

3. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

En las etapas iníciales de un proyecto como parte de los riesgos asociados al mismo, se incluye una identificación y evaluación de riesgos de seguridad de la información, para los cuales se definen controles de seguridad que aportan a su mitigación, de acuerdo con lo definido en la metodología de riesgos establecida en el grupo empresarial.

La responsabilidad sobre la implementación y la efectividad de los controles de seguridad es del gerente del proyecto y/o el dueño del proceso al cual pertenezca el proyecto con las áreas técnicas y de seguridad de la información.

4. SEGURIDAD DE LAS APLICACIONES EN REDES PÚBLICAS / PROCESAMIENTO CORRECTO EN LAS APLICACIONES

La validación de los datos de entrada y salida se realizan en los ambientes de prueba; cuando ya se encuentran verificados se colocan en el ambiente de producción del grupo empresarial.

Validación de los datos de entrada

Se implementan controles para asegurar la validez de los datos que se ingresan a los sistemas de información, teniendo en cuenta:

- Validación a nivel individual: esto comprende los tipos de datos, datos obligatorios, longitud del campo, rangos de razonabilidad, conjuntos de valores válidos, despliegue protegido de valores. La validación de entrada de datos se hace de manera automática por parte del mismo software que detectará entradas erradas de datos o no coincidentes en los campos de captura mostrando mensaje de error al usuario, el cual no contiene información detallada del error presentado.
- Ejecución de procedimientos automáticos de respuesta ante errores de validación, a través de mensajes de error al usuario.
- Registro de las actividades de ingreso de datos.
- Definición de responsabilidades para todo el personal que participa en el proceso de entrada de datos.

Control de procesamiento interno

Se implementa para asegurar la integridad de los datos en el procesamiento; para ello se selecciona entre:

- Mecanismos que validen la ejecución lógica del procesamiento.
- Validaciones para que los procesos implícitos en el software de aplicación se ajusten a los procedimientos aprobados.

Protección contra ataques a los sistemas de información empleando técnicas de desbordamiento.

- Generación automática de reportes de inconsistencias (Logs) presentadas durante el procesamiento.

Transferencia de información

Todos los mensajes sensibles de acuerdo con la clasificación de la información enviados por correo electrónico y por las aplicaciones del grupo empresarial tienen un mecanismo de cifrado digital y/o controles para evitar el acceso no autorizado a esta información.

Validación de los datos de salida

Se implementan en la etapa de desarrollo de los sistemas los controles necesarios para validar los datos de salida del sistema y asegurar el correcto procesamiento:

- Mecanismos para generar en forma automática o manual los reportes que genera el sistema.
- Clasificación de la información para identificar los destinatarios de esta y poder aplicar los controles respectivos a la información reservada y confidencial.

5. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

Los cambios cumplen con lo estipulado en las directrices de gestión de operaciones y comunicaciones.

Se mantienen los registros (logs) actualizados sobre los niveles de autorización acordados y que los mismos sean realizados por el personal autorizado.

Se identifican e implementan los controles necesarios para que en el desarrollo de software se mitiguen riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Se realizan pruebas de seguridad de la información y ciberseguridad mediante el escaneo de vulnerabilidades al código fuente desarrollado a la medida, tanto en las fases de pruebas como en producción, y que esté: (i) directamente relacionado con el objeto social de la compañía y/o (ii) administre información clasificada como confidencial en cualquier plataforma incluyendo APPs y Web para mitigar el riesgo de ciberseguridad. Para estas pruebas se utilizan como guía las mejores prácticas de OWASP.

La vicepresidencia de tecnología tiene como responsabilidad:

- Implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios que tenga definido.

- Asegurar que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- Generar, adoptar o recomendar metodologías para la realización de pruebas al software desarrollado que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

- Asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con los parches generados para las versiones en uso y que estén ejecutando una versión soporte vigente por el fabricante. Cuando la actualización pueda implicar una afectación importante a la funcionalidad del sistema se podrá aplicar una excepción después de un análisis de riesgos y con las aprobaciones que apliquen y su debida documentación.

- Asegurar que las aplicaciones y desarrollos se diseñen y construyan en versiones vigentes y estables emitidas por el fabricante respecto a las herramientas, componentes, sistemas operativos y lenguajes de programación.

- Almacenar las copias de seguridad del código fuente cuando la propiedad sea del grupo empresarial de manera segura previendo riesgos asociados a pérdida de disponibilidad, confidencialidad o integridad. En caso de que el código fuente lo almacene un tercero establecer dicha responsabilidad a nivel contractual y hacer seguimiento al cumplimiento de esta disposición.

- Aplicar el procedimiento de control de cambios a los cambios para los sistemas de información del grupo empresarial.

- Solucionar o remediar las vulnerabilidades de seguridad y ciberseguridad encontradas en el código fuente desarrollado, que sean detectadas tanto en el ambiente de pruebas como de producción, incluyendo APPs y Web, así como los diferentes servicios de soporte e infraestructura.

6. CONTROL DE CAMBIO EN SISTEMAS

Para los cambios, actualizaciones, o reconfiguraciones que puedan tener un impacto importante en los servidores de aplicaciones, de bases de datos, u otros equipos asociados a la operación de sistemas de información, se aplica el procedimiento de gestión de cambios en el que se evalúe los potenciales impactos y riesgos que puedan generar estos cambios para una adecuada planificación y ejecución.

Cada vez que sea necesario realizar un cambio significativo en el Sistema Operativo que pueda impactar los servicios, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se tiene en cuenta:

- Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

- Garantizar que los cambios en el sistema operativo sean informados con antelación a la implementación para efectos del análisis que se menciona en este numeral.

Para estos efectos la vicepresidencia de tecnología cuenta con un procedimiento que define las actividades que atienden lo indicado en este numeral.

7. RESTRICCIONES EN LOS CAMBIOS DE LOS PAQUETES DE SOFTWARE

En caso de requerir la modificación, actualización o ajuste de paquetes de software (Incluidos los paquetes suministrados por proveedores) y contando con previa autorización del responsable del activo de información:

- Analiza los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas y pueden ser realizadas.
- Retiene el software original realizando los cambios sobre una copia perfectamente identificada y documentando los cambios por si fuera necesario para aplicarlo a nuevas versiones o deshacer (“rollback”) los cambios realizados.
- En la aplicación del procedimiento de gestión de cambios, se asegura la remediación de las vulnerabilidades de seguridad y ciberseguridad encontradas, de acuerdo con lo definido en el Procedimiento de Gestión de Vulnerabilidades.

8. SEPARACIÓN DE AMBIENTES

Se mantienen los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda la plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.

Los usuarios utilizan diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se asegura que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.

Las pruebas, instalaciones o desarrollos de software requeridos son realizados en ambientes de desarrollo y pruebas, con el fin de evitar riesgos asociados a disponibilidad o confidencialidad de la información.

No se copia información sensible desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, se implementan controles para garantizar la confidencialidad de la información y esta se elimina de forma segura después de su uso.

Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor. En caso de que se solicite una excepción sobre este particular, la vicepresidencia de tecnología escalará el caso al oficial de seguridad de la información para evaluar los riesgos, establecer su viabilidad y medidas de control.

9. PRINCIPIOS DE DESARROLLO

Todo desarrollo (interno o contratado con terceros) que se realice en el grupo empresarial debe cumplir con los siguientes principios, según corresponda:

9.1 Principios de desarrollo interno en el grupo empresarial.

- Partir siempre de un modelo de permisos mínimos e ir escalando privilegios por demanda de acuerdo con los perfiles establecidos en las etapas de diseño.
- Si se utiliza un lenguaje que no sea compilado, asegurarse de limpiar el código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.
- Si se utiliza un lenguaje compilado, se debe garantizar que la compilación se realiza utilizando las mejores optimizaciones disponibles y que no se incluya información para depuración.
- Se deben incluir pruebas de cubrimiento del código para garantizar que todo el código es probado.
- La seguridad se debe incluir en el diseño de todas las capas de arquitectura (negocio, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad digital, con la necesidad de accesibilidad. De esta forma se evita tener porciones de código que resultan innecesarias.

- Validar siempre los datos que ingresan a la aplicación para garantizar que lo que está ingresando a los sistemas es lo esperado y además evitar inyecciones de código.
- Cualquier funcionalidad, campo, botón o menú nuevo debe agregarse de acuerdo con los requerimientos de diseño.
- Hacer seguimiento de las tecnologías utilizadas para el desarrollo, a fin de garantizar su mantenimiento en la última versión vigente.
- Todos los accesos que se hagan a los sistemas son validados.
- Para intercambiar información sensible utilizar protocolos para cifrar las comunicaciones, utilizando algoritmos fuertes y claves robustas
- Cualquier cambio que se haga queda documentado, esto facilitará modificaciones futuras.
- Generar planes de remediación a las vulnerabilidades confirmadas con criticidad muy alta o alta.
- Como parte de las actividades del ciclo de vida del desarrollo SDL se deben tomar como referencia las prácticas reconocidas de desarrollo seguro, por ejemplo: Microsoft SDL, OWASP, SANS CWE Top 25, CERT Secure Coding.
- Haber pasado por un proceso completo de pruebas (técnicas, funcionales, cargas y estrés, seguridad, etc.) y certificación los sistemas de información del grupo empresarial, antes de ser liberados a producción en un ambiente dedicado para tal fin.

9.2 Principios de desarrollo contratados a terceros

Cuando los desarrollos se contraten con terceros, la vicepresidencia de tecnología valida los principios de desarrollo que tenga definido el tercero.

Todos los contratos de desarrollo con terceros deben incluir los principios de desarrollo seguro del tercero y los que defina el grupo empresarial a nivel contractual, en el numeral de obligaciones del tercero.

ANEXO No. 3 – POLITICA INTERNA DE CONTROL DE ACCESOS

ALCANCE/APLICABILIDAD

La información contenida en el presente documento es de aplicación exclusiva para la organización y de uso de los responsables asignados para cada una de las empresas que conforman el grupo empresarial, según corresponda.

RESPONSABILIDADES

Las siguientes directrices aplican a todo el personal y/o terceros que administre y/o los sistemas de información del grupo empresarial.

DIRECTRIZ GENERAL

Todo mecanismo a través del cual se procese y almacene información del grupo empresarial debe cumplir con las directrices y procedimientos de control de acceso.

1. REQUISITOS PARA EL CONTROL DE ACCESO A LA INFORMACIÓN

Los colaboradores y terceros autorizados del grupo empresarial tienen acceso exclusivamente a la información que por ejercicio de sus funciones y actividades dentro del grupo empresarial así lo requieran, es decir, teniendo en cuenta los principios de necesidad de conocer (need-to-know, NtK) y mínimo privilegio (least privilege, LP). La asignación de los privilegios y accesos deben estar basadas en las necesidades de cada área y ser aprobados por el propietario de cada activo.

Estas necesidades de acceso son determinadas por las respectivas vicepresidencias, direcciones o coordinaciones en función de las tareas asignadas a cada colaborador, las cuales conservan la trazabilidad requerida y quedan registradas en el sistema de soporte (mesa de ayuda).

Los accesos a terceros sólo son otorgados previa solicitud del propietario del activo o sistema de información y siempre previo acuerdo de confidencialidad firmado entre las partes. Para este fin se realiza una validación por el Oficial de Seguridad de la Información, quien da la autorización para la asignación de accesos y se actualiza la matriz de control accesos para que las nuevas solicitudes se ejecuten directamente. Las cuentas de acceso a terceros tienen especificado un tiempo de expiración (cuando aplique), el cual es controlado por el administrador del sistema o la VP. Digital, según aplique.

En caso de requerirse un acceso con perfil administrador en cualquier ambiente, aplicación y/o servicio, este debe contar previamente con la autorización del Oficial de Seguridad de la Información, a quien se le indicará la justificación correspondiente para realizar la actividad.

El oficial de seguridad de la información tiene las facultades de solicitar la suspensión o eliminación de los accesos a cualquier persona que represente un riesgo frente a la confidencialidad, disponibilidad y/o integridad de la información; en los casos que esta suspensión o eliminación derive de la materialización de un incidente de seguridad, este se registrará como tal y se llevará a cabo el correspondiente proceso disciplinario.

Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, medios de procesamiento, sistemas o información es considerado un incidente grave, por lo que debe reportarse de inmediato de acuerdo con el procedimiento de gestión de incidentes de seguridad de la información y ciberseguridad y se iniciará un proceso disciplinario sobre las personas que realizaron dicha actividad.

2. CONTROL DE ACCESOS

Identificación y Autenticación es la primera línea de defensa y es la base para los controles de acceso y para el seguimiento de las actividades de los usuarios. Será implementado a través de un mecanismo de autenticación sobre el cual los usuarios se identifican y que se encarga luego de validar al usuario sobre los recursos a los que éste pueda acceder.

El control de acceso a los sistemas de procesamiento y almacenamiento de información del grupo empresarial se realiza por medio de cuentas únicas para cada usuario, por lo que las cuentas de usuario y claves de acceso son personales e intransferibles.

La administración de los usuarios de los sistemas misionales y financieros son llevada a cabo por la Dirección/ coordinación responsable, específicamente por el colaborador que asuma el rol de Administrador del Sistema, quien en desarrollo de esta actividad atiende las directrices contenidas en este documento.

Los usuarios internos del grupo empresarial podrán ingresar a los sistemas de carácter misional, previo cumplimiento del procedimiento establecido para este fin por el respectivo administrador, en lo referente a la solicitud de usuarios y sólo para efectos de desempeñar las actividades inherentes al cargo que desempeñan en la entidad.

Si el sistema de acceso no funciona correctamente es responsabilidad de quien encuentre tal inconsistencia informar al administrador del sistema a través del sistema de soporte (mesa de ayuda).

Los controles de accesos definen los perfiles o privilegios de acceso de los usuarios a las aplicaciones de acuerdo con su rol en la organización, los cuales están documentados en las matrices de roles y perfiles o tablas de derechos de acceso correspondiente a cada sistema, aplicación, etc.

3. GESTIÓN DE PRIVILEGIOS

Los administradores de los sistemas de información mantienen los registros donde cada uno de los líderes responsables de los procesos o directores, haya autorizado a los colaboradores de la organización y/o terceros el acceso a los diferentes sistemas de información de la organización.

Todos los usuarios son previamente registrados antes de acceder a cualquier sistema de información del grupo empresarial. Los datos de acceso a los sistemas de información están compuestos por un ID o nombre de usuario y contraseña que es único para cada colaborador o tercero.

Todo sistema de información tiene asignado un administrador del sistema quién garantiza el buen uso del sistema y la administración de acceso al mismo.

4. REVISIÓN DE DERECHOS DE ACCESOS

La Vicepresidencia de tecnología es la responsable de los accesos a las bases de datos, infraestructura y sistemas de información bajo su responsabilidad, así como las otras áreas del grupo empresarial sobre los sistemas bajo su responsabilidad, de tal forma que se establezca un control efectivo desde el registro inicial de la cuenta hasta el momento en que requiera ser modificada, revocada o eliminada.

Los derechos de acceso son revisados:

- Trimestralmente por los administradores de cada sistema a fin de garantizar que los perfiles asignados y los usuarios existentes tengan acceso a la información para efectos de desempeñar las actividades inherentes al cargo que desempeña en la entidad. La Dirección de riesgos realiza trimestralmente un monitoreo de los usuarios y perfiles de acceso a los sistemas de información Core del grupo empresarial, el administrador de la aplicación o del sistema debe tener un control de segregación de funciones a través de una matriz que asegure la correcta asignación del rol y perfil a los usuarios del sistema.

  Si se requiere crear un nuevo perfil o modificar los que ya están creados, se debe hacer la verificación entre el administrador de la aplicación o del sistema con el área solicitante, acotando las necesidades de acceso del usuario, cuando ya se defina el rol y el perfil, para hacer la modificación en esa matriz de roles y perfiles se debe validad que cumpla el criterio de segregación de funciones acorde a lo solicitado por la operación, para que se garantice la labor del ejecutor del control de acceso.

- Después de cualquier cambio mayor en la organización

5. MONITOREO DE ACCESO

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica, la dirección de riesgos realizará un seguimiento a los accesos realizados por los usuarios a la información del grupo empresarial, con el objeto de minimizar el riesgo de pérdida de integridad de la información.

Cuando se presenten eventos que pongan en riesgo la integridad, disponibilidad y/o confidencialidad de los activos de la información se documentan y realizan las acciones que

permitan su solución de acuerdo con el procedimiento de gestión de incidentes del grupo empresarial.

6 DIRECTORIO ACTIVO

6.1 MODALIDAD DE ACCESO

La Vicepresidencia de tecnología establece en el Directorio Activo los permisos asignados a Usuarios sobre los recursos compartidos (Carpetas e Impresoras, Share point, One Drive Email) y a la información, de acuerdo con la solicitud en el sistema de soporte (mesa de ayuda) que realice el Director, Gerente, Gerente Corporativo o Vicepresidente responsable de los procesos, previa validación del Oficial de Seguridad de la Información, a fin de garantizar la correspondiente segregación de funciones, lo cual queda registrado en la matriz de control de accesos para que las nuevas solicitudes se ejecuten directamente.

Los permisos de accesos se definen de la siguiente forma:

- Lectura: el usuario podrá únicamente leer o visualizar la información, pero no podrá editarla. Debe considerarse que la información podrá ser copiada o impresa.
- Escritura: este tipo de acceso permitirá agregar datos, modificar o borrar información.
- Ejecución: este acceso otorgará al usuario el privilegio de ejecutar programas.
- Borrado: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- Control Total: el usuario podrá modificar los permisos anteriormente descritos.
- Creación: permite al usuario crear nuevos archivos, registros o campos.
- Búsqueda: permite listar los archivos de un directorio determinado.

6.2 UBICACIÓN Y HORARIO

El acceso a determinados recursos del sistema se basa en la ubicación física o lógica de los datos o usuarios.

Para garantizar el respaldo de la información, los colaboradores almacenan dicha información en los medios dispuestos por la Vicepresidencia de tecnología para tal actividad.

6.3 NOMBRE DE USUARIO

Los usuarios de directorio activo son identificados por la forma: inicial del primer nombre seguido del primer apellido completo (p.a. para Pedro Pérez el usuario deberá ser Pérez).

- En los eventos en que ya exista un usuario con un nombre igual, se asignará la primera letra del segundo nombre.
- No se permitirán nombres de usuario con tildes, mayúsculas y la letra "*ñ*" se deberá cambiar por n.
- No se considerarán los enlaces, por ejemplo, en *Maria del valle* no se tiene en cuenta "*del* ".
- Si dos o más personas tienen el mismo nombre de usuario, se añadirá al segundo y posterior la primera letra del segundo apellido.

7. REVOCACION, DESACTIVACIÓN O MODIFICACIÓN DE LOS ACCESOS

Por terminación del contrato laboral la dirección de talento y cultura solicitará la desactivación del usuario de dominio del colaborador por medio del sistema de solicitud de soportes, adicionalmente informará formalmente a la Dirección de Tecnología y las demás áreas que tengan administración de aplicativos del grupo empresarial y demás sistemas, una vez se presente la desvinculación de un colaborador.

En el momento que el colaborador termine su relación laboral con el grupo empresarial, todos los permisos de accesos a los sistemas de información son revocados inmediatamente y de manera permanente.

Cuando se presenten ausencias del colaborador iguales o mayores a seis (6) días por vacaciones, licencias, permisos o incapacidad, se bloqueará temporalmente los accesos hasta que se incorpore nuevamente a sus actividades. La Dirección/coordinación a la que pertenezca el colaborador es la responsable de informar de la ausencia a la dirección de talento y cultura quien centraliza la solicitud de desactivación/activación de los accesos del usuario, a través del sistema de soporte. Toda ausencia o novedad de los terceros o proveedores, debe ser reportado inmediatamente por parte del responsable del contrato a los responsables de administrar las plataformas o sistemas de información para que realicen los respectivos bloqueos de acceso.

Cuando se presente el cambio de cargo de un colaborador dentro del grupo empresarial, se hace necesario revisar los permisos de acceso lógico asignados y verificar su validez de acuerdo con su nuevo rol, las modificaciones son solicitadas por el director/coordinación de la Dirección/coordinador la que pertenece el colaborador antes del cambio de rol a través del sistema de soporte.

Cuando el líder del proceso solicite permisos de acceso temporales a los sistemas de información del grupo empresarial, a su personal a cargo, (sea del grupo empresarial , outsourcing o proveedores), es responsabilidad del líder garantizar que una vez finalice la actividad o tarea se le retire o desactive el permiso temporal. La solicitud de desactivación del permiso temporal se realiza por la mesa de ayuda

Los accesos serán desactivados por manejo indebido de la información, de acuerdo con la auditoría sobre el log de actividades realizadas por el Usuario de acuerdo con lo definido en el Procedimiento de Gestión de Incidentes y en caso de materializar un incidentes o evento, este es informado para realizar el correspondiente análisis y de ser necesario aplicar el correspondiente proceso disciplinario.

Para la aplicación SIB por defecto se asignarán los usuarios con una caducidad y renovación de forma anual, teniendo en cuenta que se ejecutarán los siguientes controles por parte de la administración del aplicativo, el cual será objeto de revisión por los entes de control interno:

- La vigencia de acceso al sistema debe ser de un año para todos los usuarios a partir de la implementación de la regla y los usuarios creados posteriormente.

- Teniendo en cuenta que la administración de estos accesos la realiza la Dirección de Producción e Infraestructura debe garantizar una revisión periódica de los usuarios activos los cuales deben coincidir con los que se encuentran en nómina para usuarios internos y que concuerden con los terceros autorizados por el área de Operaciones y/o este designado para la realización de solicitudes de accesos al sistema SIB.

8. GESTIÓN DE CONTRASEÑAS

Cada usuario tiene un único ID o nombre de usuario y contraseña de acceso, los cuales es de uso personal e intransferible.

El sistema operativo entrará en estado de suspensión a partir de 10 minutos de inactividad del usuario.

Toda contraseña que entregue el respectivo administrador del sistema deberá ser cambiada por el usuario luego de ingresar al sistema por primera vez.

Las palabras claves o contraseñas de acceso a los recursos informáticos, que sean asignadas a los colaboradores del grupo empresarial serán de responsabilidad exclusiva de cada uno de ellos y no pueden ser divulgados o transferido. Los usuarios serán responsables de todas las actividades llevadas a cabo con su usuario y sus claves asignadas.

Para los sistemas misionales y financieros del grupo empresarial, se entrega una contraseña ~~la~~ genérica. El sistema forzará el cambio de la contraseña en el siguiente inicio de sesión el lapso para este cambio es de 24 horas, atendiendo los parámetros de configuración de contraseña, la cual será cifrada por el sistema, de manera que sólo la conocerá el usuario y responsabilidad de su buen uso acorde a la responsabilidad asignada en la organización.

Las contraseñas en los sistemas de información que administra el grupo empresarial, independientemente de su naturaleza, les solicita cambio como mínimo cada 45 días.

Las contraseñas establecidas por los proveedores son cambiadas inmediatamente después de que el sistema se ponga en producción siempre y cuando no se vea afectada la funcionalidad del sistema y de acuerdo con el análisis de riesgo correspondiente.

Todo usuario que tenga sospecha que su contraseña es conocida por otra persona, debe cambiarla inmediatamente.

En los sistemas misionales y financieros del grupo empresarial se tiene establecido un control de tres intentos consecutivos fallidos de ingreso al sistema que produzca el bloqueo de la cuenta por un tiempo predeterminado de 10 minutos.

Historial de contraseñas: El sistema siempre y cuando lo permita, guardará el historial de las últimas 24contraseñas utilizadas y el usuario no podrá disponer de ellas durante el tiempo que se defina.

Cambio de contraseña: en caso de olvido de la contraseña, el usuario de cada Dirección/coordinación solicita registrará la restauración de la contraseña a través de la mesa de ayuda al área de soporte de la Dirección de Producción e infraestructura o los medios tecnológicos autorizados por esta Dirección.

En los sistemas SIG y SIB, el cambio de contraseña lo hacen directamente los usuarios mediante la opción de “cambio de contraseña” o de “olvido su contraseña”.

Las contraseñas deben tener mínimo 8 caracteres y máximo 144, combinar letras mayúsculas, minúsculas, caracteres especiales y números, se recomienda no usar nombres del usuario o familiares del usuario, apellidos ni meses del año.

Está prohibido almacenar contraseñas en libretas, cuadernos y demás medios físicos o en medios electrónicos o digitales sin tener un cifrado controlado por el usuario al que se le asignan las credenciales y autorizado por seguridad de la información.

Se prohíbe crear identificaciones de usuarios en el dominio genéricos a excepción de cuentas de servicio o cuentas de grupos/buzones de correos, basados en sus funciones de trabajo, a excepción de procesos automáticos cuyo origen son aplicativos misionales y las cuentas de correo de las comunicaciones corporativas del grupo empresarial.

Todos los aplicativos o sistemas productivos de la organización que no se encuentren bajo las políticas del directorio activo, deben cumplir los lineamientos de gestión de contraseñas, no obstante, si la capacidad del software impide su cumplimiento se debe tener una justificación por cada uno de los apartados del numeral 4.8 y el dueño del aplicativo debe proponer los controles de seguridad de la información que debe ser aprobados por Seguridad de la Información.

9. USUARIOS EXTERNOS

- Los usuarios externos del SIB y SIG, serán las Sociedades Comisionistas de Bolsa (SCB) y las entidades de control como la Superintendencia Financiera, la Contraloría General de la República y la Revisoría Fiscal y proveedores que requieran el acceso a ambientes de desarrollo o pruebas para el desarrollo del objeto de su contratación.

- Los usuarios externos del sistema Electrónico para el Gestor del Mercado de Gas (SEGAS), serán las entidades participantes del mercado de gas natural en Colombia, la CREG y otros usuarios autorizados en virtud del convenio.

- La Sociedad Comisionista de Bolsa deberá presentar mediante comunicación escrita y firmada por el representante legal, la solicitud de creación del Usuario en el sistema misional para efectos de desempeñar las actividades requeridas para el desarrollo de su objeto social y que estén relacionadas con la operación en Bolsa Mercantil. En esta comunicación se deberá especificar el perfil requerido para el miembro de la SCB.

- Los usuarios con el perfil Comisionista, sólo podrán consultar y modificar la información de la SCB a la cual pertenezcan, preservando el principio de reserva bursátil.

- La clave asignada al usuario se entregará por medio de correo electrónico; el correo enviado deberá contener la siguiente estructura: El correo debe contener la comunicación en PDF, que contenga el usuario y clave asignados, con clave para apertura del archivo (esta clave se informará verbalmente o por otro medio distinto al correo electrónico en el que se envía el PDF).

- El buen uso del usuario y clave será responsabilidad de la Entidad quedando prohibido el préstamo de estos elementos para permitir el ingreso al sistema a personas ajenas a la Entidad, y recaerá bajo su responsabilidad la propagación, pérdida o manipulación indebida de la información en caso de que esto ocurra.

- Los perfiles de Usuario podrán ser modificados previa notificación de la solicitud a través de comunicación escrita firmada por el representante legal, donde se justifique la modificación de los permisos y accesos del Usuario. La modificación del perfil de un Usuario contempla adicionar o quitar permisos sobre las opciones de menú y de las tablas del sistema o el cambio de grupo del usuario.

- Los usuarios se desactivarán en los siguientes casos:

    - Por solicitud escrita de la Entidad o Sociedad Comisionista de Bolsa.
    - Por manejo indebido de la información, en cuyo caso se reporta el correspondiente evento o incidente de seguridad.
    - Por pérdida de la calidad de SCB ante la Bolsa Mercantil. En este caso la inactivación de todos los usuarios asignados es permanente.

- Para el caso de los entes de control como la Superintendencia Financiera de Colombia y la revisoría fiscal, la Auditoría Interna o quien la Presidencia designe presenta la solicitud mediante comunicación escrita a la Vicepresidencia de tecnología o el área administradora de aplicaciones, indicando la justificación del usuario. Dichos usuarios sólo tendrán acceso para consultar la información, de manera que les permita llevar a cabo sus funciones de vigilancia y control.

10. VPN

La administración de los usuarios VPN es llevada a cabo por la Vicepresidencia de tecnología.

El uso de VPN será asignado para efectos de la ejecución de las modalidades de trabajo en casa y teletrabajo de acuerdo con la directriz establecida para este fin por parte del grupo empresarial. Igualmente, para permitir conexiones de terceros que se requiera para el desarrollo del objeto de los contratos y el uso de los servicios del grupo empresarial.

El Administrador de Redes o quien desempeñe su función, configurará el perfil del usuario que requiere el colaborador, previa autorización del director o Gerente del área, de acuerdo con las labores que desempeña el solicitante.

El uso del usuario y clave es personal e intransferible, es decir, el colaborador en ningún caso podrá prestar su usuario y clave para permitir el ingreso al sistema a otro colaborador ni a personal externo

de la Entidad, y recaerá bajo su responsabilidad la propagación, pérdida o manipulación indebida de la información en caso de que esto ocurra.

Los usuarios se desactivarán en los siguientes casos:

- Por cambio en las funciones que desempeña el colaborador. En este caso se ajustarán los permisos asignados.
- Por ausencia del colaborador por vacaciones, licencias. En este caso la inactivación será temporal hasta que el usuario se incorpore nuevamente a sus actividades.
- Por manejo indebido de la información, de acuerdo con la auditoría sobre el log de actividades realizadas por el usuario.
- Por retiro de la entidad. En este caso la inactivación será permanente.

Para que la desactivación sea procedente, esta es notificada a la dirección de talento y cultura mediante el registro de la solicitud en el Sistema de Soporte, la razón de la inactivación del usuario; para que la Dirección de Tecnología realice las actividades pertinentes.

La solicitud de creación para usuarios VPN de terceros es realizada por medio de un correo electrónico dirigido a la Dirección de Tecnología; estas solicitudes deben ser remitidas por el Representante Legal de la SCB. La respuesta a esta solicitud se realiza por medio de correo electrónico; en el correo se informará como mínimo lo siguiente:

- Para las Sociedades Comisionistas de Bolsa el correo será remitido al correo electrónico del Representante Legal de la SCB.
- Comunicación en PDF, que contenga el usuario y clave asignados, con clave para apertura del archivo.
- La clave de apertura es una contraseña aleatoria que cumpla con la directriz de contraseñas seguras.
- La clave asignada requerirá cambio de esta en primer inicio de sesión.

10.1 USUARIOS VPN

- La estructura del usuario para usuarios internos o externos está conformada de la siguiente forma: primer nombre seguido del primer apellido completo, separado con punto (p.o. pedro. Pérez). En los eventos en que ya exista un usuario con un nombre igual, se asignará la primera letra del segundo apellido. Para el caso de la SCB la estructura del usuario será de la forma: comixx_yy, donde xx corresponde al número que identifica la SCB y yy corresponde al número de usuario de VPN. Para el soporte de proveedores se podrán manejar usuarios genéricos dependiendo de la necesidad.

- No se permiten tildes, mayúsculas, y la letra ñ se deberá cambiar por n.

- Los usuarios de las cuentas de VPN de las Sociedades Comisionistas de Bolsa son revisados trimestralmente por el Administrador, con la información suministrada por la Vicepresidencia de Operaciones, a fin de garantizar que sólo accederán a los recursos, las Sociedades Comisionistas de Bolsa y las entidades de control.

Las cuentas de VPN de proveedores y/o entes de control, el responsable de notificar las novedades de creación y eliminación es del director o gerente encargado del proceso y/o contrato a través de una solicitud en el aplicativo de soporte.

11. PERSONAL EXTERNO Y ENTES DE CONTROL

Si el personal externo y colaboradores de los entes de control necesitan ingresar a las instalaciones del grupo empresarial recursos informáticos que no sean de propiedad del grupo empresarial , y/o conectarse a los sistemas de información del grupo empresarial , , estos elementos tienen que ser revisados por parte de la Dirección de Tecnología del grupo empresarial , para poder autorizar su ingreso y funcionamiento dentro del grupo empresarial y/o conexión a la red; razón por la cual previo al ingreso de los elementos, se solicitará al personal externo y colaboradores de los entes de control la autorización para llevar a cabo la revisión de los elementos que ingresan, para ello se les solicitará un inventario de los equipos a ingresar, los tiempos de permanencia dentro del grupo empresarial y la actividad a realizar.

Para la conexión a la red de los sistemas de información se debe tener la autorización del Oficial de seguridad de la información.

Estos usuarios tendrán acceso a los recursos informáticos que sean estrictamente necesarios para el cumplimiento de su función; los servicios son aprobados y solicitados por quien se desempeñe como superior inmediato o director o gerente, o en su caso, por el colaborador del grupo empresarial que el presidente designe para coordinar las labores de inspección del respectivo ente de control. En todo caso, deberán firmar el acuerdo de buen uso de los recursos informáticos.

12. CONTROL DE ACCESO SHAREPOINT POR PROCESO – SHAREPOINT COMPARTIDO - ONE DRIVE OFFICE 365

A continuación, se describen las políticas de control de acceso a los servicios cloud de Sharepoint y One Drive de Office 365.

One Drive:

El grupo empresarial define que el servicio de One Drive Office 365 es para almacenamiento de información exclusivo para cada usuario o colaborador de la organización.

Cada One Drive tiene acceso por una única cuenta asociada al ID del usuario en el Directorio Activo.

El colaborador es responsable de su One Drive y no deben compartir su carpeta a otros usuarios o colaboradores del grupo empresarial, terceros o hacia internet.

SHAREPOINT POR PROCESO

El objetivo del Sharepoint por proceso es que únicamente tengan acceso los colaboradores que hacen parte de un proceso.

El responsable de autorizar los accesos de los usuarios al Sharepoint del proceso es el líder responsable del Proceso.

Los usuarios o colaboradores con acceso al Sharepoint por proceso, no pueden compartir su carpeta, archivos u otro tipo de información a otros usuarios o colaboradores del grupo empresarial, terceros o hacia internet ajenos al proceso.

SHAREPOINT COMPARTIDO

El objetivo del sharepoint compartido es para que colaboradores de diferentes procesos puedan intercambiar información, relacionada con proyectos, iniciativas, etc. evitando el acceso al Sharepoint del proceso. También aplica acceso a los externos (proveedores, outsourcing, reguladores, etc.)

Cada colaborador de la organización puede solicitar la creación de un sharepoint compartido, siempre y cuando tenga la aprobación de su líder. En la solicitud se tiene que indicar: tipos de acceso que tendrán los otros colaboradores y tercero, los tipos de permisos: Lectura, escritura y/o borrado y el tiempo por el cual se requiere.

Los usuarios o colaboradores/Terceros con acceso al Sharepoint Compartido, no pueden compartir su carpeta, archivos u otro tipo de información a otros usuarios o colaboradores del grupo empresarial, terceros o hacia internet.

13. MATRIZ DE ACCESOS A SERVICIOS DE RED, SEGURIDAD, SISTEMAS DE INFORMACIÓN PARA USUARIO FINAL

A continuación, se relaciona el listado de los servicios que ofrece la compañía, el cual se incluyen requisitos de seguridad y controles de accesos a colaboradores, terceros (clientes, proveedores, etc.)

Servicio	Tipo de Usuario	Mecanismo de Autenticación	Autorización	Controles adicionales
AWS	Colaborador VP de tecnología	Usuario y contraseña + Segundo factor de autenticación Token / OTP	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)

Servicio	Tipo de Usuario	Mecanismo de Autenticación	Autorización	Controles adicionales
	Colaborador	Usuario y contraseña + Segundo factor de autenticación Token / OTP	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Proveedores	Usuario y contraseña + Segundo factor de autenticación Token / OTP	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y evaluación de seguridad de la información (proveedores críticos que les aplique)
Office 365	Colaborador VP. Digital	Usuario y contraseña + Segundo factor de autenticación Token / OTP	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Colaborador	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad
	Proveedores	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y evaluación de seguridad de la información (proveedores críticos que les aplique)
Core Swicth	Colaborador VP de tecnología	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
Firewall (Teleport)	Colaborador VP de tecnología	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Colaborador (colaboradores del área de riesgos)	Usuario y contraseña	Solo aplica para consulta - requiere autorización del oficial de seguridad de la información	Contrato cláusula de confidencialidad

Servicio	Tipo de Usuario	Mecanismo de Autenticación	Autorización	Controles adicionales
VPN	Colaborador VP de tecnología	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Colaborador	Usuario y contraseña	Solo para ingreso a la red de la organización - Autoriza Líder de área	Contrato cláusula de confidencialidad
	Proveedores	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y evaluación de seguridad de la información (proveedores críticos que les aplique)
Switches Redes	Colaborador VP de tecnología	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Proveedores	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y evaluación de seguridad de la información (proveedores críticos que les aplique)
Aplicaciones Core del Negocio (SIG, SIB, SEGAS, Etc.)	Administradores plataforma	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Colaboradores	Usuario y contraseña	Perfil de acuerdo con rol y funciones del cargo/proceso - Autoriza Líder de área	Contrato cláusula de confidencialidad
	Clientes finales /otros Terceros	Usuario y contraseña	Perfil de acuerdo con tipo de tercero - Autoriza la operación	Contrato cláusula de confidencialidad

Servicio	Tipo de Usuario	Mecanismo de Autenticación	Autorización	Controles adicionales
Directorio Activo - Red	Colaborador VP de tecnología	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Colaborador	Usuario y contraseña	Solo para ingreso a la red local de la organización - Autoriza Líder de área	Contrato cláusula de confidencialidad
	Proveedores	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y evaluación de seguridad de la información (proveedores críticos que les aplique)
Plataformas de Ciberseguridad	Colaborador VP de tecnología	Usuario y contraseña + Segundo factor de autenticación Token / OTP	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Colaborador	Usuario y contraseña + Segundo factor de autenticación Token / OTP	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Proveedores	Usuario y contraseña + Segundo factor de autenticación Token / OTP	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y evaluación de seguridad de la información (proveedores críticos que les aplique)
Servidores e Instancias en AWS y Servidores Centro de datos Teleport	Colaborador VP de tecnología	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)
	Colaborador	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y estudio de seguridad previo al ingreso (Talento Humano)

Servicio	Tipo de Usuario	Mecanismo de Autenticación	Autorización	Controles adicionales
	Proveedores	Usuario y contraseña	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y evaluación de seguridad de la información (proveedores críticos que les aplique)
Internet WIFI Invitados	Invitados	Contraseña wifi Internet red de invitados	Líder de proceso	
Conexión de equipos de terceros para pruebas (concepto, Demo)	Proveedores	Usuario y contraseña de red	Privilegio de administrador requiere autorización del Oficial de seguridad de la información	Contrato cláusula de confidencialidad y evaluación de seguridad de la información (proveedores críticos que les aplique)

ANEXO No. 4 INTERNA DE CONTROLES CRIPTOGRÁFICOS

ALCANCE / APLICABILIDAD

La Directriz está dirigida a todos los colaboradores y demás partes interesadas del grupo empresarial.

RESPONSABILIDAES

Los dueños de la información están obligados a cumplir esta política para los casos en que las entidades regulatorias o el ejerció operativo de la organización lo requiera, información contenida en el presente documento es de aplicación exclusiva para la Bolsa o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

DIRECTRIZ GENERAL

Se utilizan controles criptográficos en los siguientes casos:

1. Para la protección de claves de acceso a sistemas, base de datos y servicios como mínimo para aquellos considerados de misión crítica para la compañía.
2. Para la transmisión de información confidencial de acuerdo con lo definido en el Manual de Procedimientos para la Gestión Documental. Cuando la información confidencial se trasmita por correo electrónico esta se protege mediante claves sobre los archivos adjuntos.
3. Para el resguardo de información, cuando así surja del análisis de riesgos, aplicando la metodología de riesgos adoptada por el grupo empresarial en políticas del sistema integral de administración de riesgos, realizado por el líder del proceso y el oficial de seguridad de la información.

4. Para el almacenamiento de las contraseñas de los sistemas operativos, gestión de identidad y bases de datos.
5. Para todo el proceso de autenticación de los usuarios en las aplicaciones Core del negocio.
6. Para la transferencia y transmisión de información confidencial a terceros (proveedores)
7. Para las trasmisiones de información con entes regulados, siempre y cuando esté acordado y/o definido en una regulación, contrato, acuerdo u otro mecanismo equivalente.
8. Para todas las aplicaciones web públicas, servicios web, API expuestas en Internet y al interior del grupo empresarial.
9. Para los servicios o aplicaciones de resguardo o bóvedas de contraseña.

Está totalmente prohibido para los colaboradores el uso de sistemas de cifrado, firmas o certificados digitales para las actividades o para los sistemas de información sin la previa autorización del oficial de seguridad de la información y de la vicepresidencia de tecnología.

A toda información confidencial se le aplican controles que mitiguen el riesgo de fuga de información y el acceso no autorizado si no se encuentra en uso activo.

La siguiente información es definida por el grupo empresarial como confidencial y sensible; por lo tanto, requiere tener implementado controles criptográficos:

- Información de clientes: información de contacto de los comitentes o mandantes, tasas de negociación, detalle de las operaciones realizadas por las comisionistas y operadores del mercado de gas.
- Información de colaboradores: todo lo relacionado con nómina y salud del colaborador.
- Información de autenticación: contraseñas de acceso, doble factor de autenticación (sistemas que lo tengan implementado), preguntas de seguridad si aplica.

En caso de transmitir grandes volúmenes de información se deben usar servicios como FTPS o SFTP, One Drive o Sharepoint de Microsoft, suministrados por la vicepresidencia de tecnología.

En caso de requerir controles criptográficos para un sistema o activo de información no contemplada en esta Directriz se debe solicitar apoyo al Oficial de Seguridad de la Información.

1. GESTIÓN DE LLAVES

Las áreas Vicepresidencia de riesgos y cumplimiento y vicepresidencia de tecnología están a cargo de la implementación de controles de cifrado sobre la plataforma informática del grupo empresarial que se encuentre expuesta en el ciberespacio, así como de la definición del tipo de cifrado apropiado para cada escenario, con el fin de proteger la información de la organización.

Las llaves criptográficas utilizadas para el cifrado de los datos están clasificadas como confidencial y son protegidas contra divulgación, uso indebido o sustitución no autorizada restringiendo al mínimo el número de custodios necesarios y guardándola de forma segura en la menor cantidad de ubicaciones y formas posibles.

Se mantienen registros de trazabilidad de las actividades de gestión de claves.

Las llaves de cifrado son información de alta sensibilidad (confidencial) y el acceso a ellas es estrictamente limitado a quienes demuestren la necesidad de saber (Need-to-Know).

La vicepresidencia de tecnología documenta el manejo y la administración de llaves de cifrado a su cargo; así mismo cualquier área del grupo empresarial que tenga bajo su administración llaves de cifrado.

Las llaves de cifrado deben estar almacenadas en un repositorio que requiera mínimo un factor de autenticación o un control de acceso para aquellos usuarios no autorizados. Si el almacenamiento se realiza en una plataforma de un Tercero (proveedor), se debe validar en su infraestructura tecnológica los controles de ciberseguridad que tiene implementado.

Las vigencias de llaves de cifrado se definen en el momento de la implementación de estas, quedando documentado en la solicitud.

Los sistemas automáticos de generación de llaves de cifrado son administrados por la vicepresidencia de tecnología.

Las llaves de cifrado privadas del ambiente producción, no se comparten con terceras partes.

2. EXCEPCIONES

En el caso que no sea posible implementar controles criptográficos en el almacenamiento y/o intercambio de información confidencial, el Oficial de Seguridad de la Información, la y el dueño del activo, valoran los riesgos, e implementar mecanismos de seguridad complementarios con el fin de que el riesgo residual sea aceptable o tramitar una solicitud de aceptación de riesgo.

ANEXO No. 5 - POLÍTICA INTERNA DE DISPOSITIVOS MÓVILES

ALCANCE

La siguiente directriz aplica para los colaboradores que a través de dispositivos móviles tengan acceso a datos o información del grupo empresarial.

La información contenida en el presente documento es de aplicación exclusiva para la Bolsa o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

RESPONSABILIDADES

La siguiente directriz aplica para los colaboradores que la organización le asigna un dispositivo móvil o tiene privilegios de acceso a través de dispositivos móviles a los recursos del grupo empresarial.

DIRECTRIZ GENERAL

Es responsabilidad de los colaboradores de la organización dar buen uso de los equipos móviles cuando estos por necesidades del servicio y de sus funciones, se utilizan fuera de las instalaciones de la organización, ante lo cual se deben mantener la misma directriz de seguridad como si estos estuvieran dentro de las instalaciones de la compañía.

Respecto de los dispositivos móviles provistos por el grupo empresarial, derivado del análisis de riesgos se contemplan como mínimo los siguientes controles:

- Asegurar los dispositivos (cuando los equipos estén desatendidos o fuera de las instalaciones) con base en los controles de seguridad definidos en el análisis de riesgos.
- Los dispositivos móviles no se dejan a la vista en el interior de los vehículos, ni desatendidos en lugares públicos.
- En caso de viaje siempre se llevan como equipaje de mano.
- En caso de pérdida o robo de un dispositivo móvil se informa inmediatamente por correo electrónico u otro medio disponible al jefe inmediato con copia a la dirección administrativa, dirección de infraestructura y la dirección de riesgos (riesgooperativosfc@bolsamercantil.com.co).
- El responsable del equipo realiza denuncia ante la autoridad competente y reporta a través de la herramienta definida para este fin el robo del equipo como un evento de riesgo operacional (ERO).
- Para los dispositivos móviles dados de baja o reasignados se ejecutan procedimientos de borrado seguro de la información.

Cuando se habiliten servicios informáticos en dispositivos móviles personales, el colaborador aplica medidas de seguridad tales como el bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón, huella dactilar, reconocimiento de voz, entre otras. Adicionalmente, se requiere el uso de antivirus y mantener actualizado el sistema operativo a las últimas versiones disponibles.

Con el objetivo de asegurar la disponibilidad y la confidencialidad de la información de la organización, se restringe el almacenamiento de información en medios locales (discos, USB, medios magnéticos), a menos que sean los propios de la organización y sean estrictamente necesarios para la ejecución de los proyectos o las actividades corrientes del colaborador. En este caso el jefe inmediato del colaborador que tendrá asignado el activo debe enviar una solicitud al oficial de seguridad de la información sustentando la necesidad de utilizar este tipo de medios de almacenamiento de información.

ANEXO No. 6 – POLÍTICA INTERNA DE ACTIVOS DE INFORMACIÓN

ALCANCE/APLICABILIDAD

Esta directriz aplica a los activos de Información del grupo empresarial.

La información contenida en el presente documento es de aplicación exclusiva para la Bolsa o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

RESPONSABILIDADES

Es responsabilidad de todos los colaboradores del Grupo empresarial bolsa mercantil hacer cumplir la política de activos de información

DEFINICIONES

- **Activo de Información:**

En el contexto de la ISO /IEC 27001 es algo que el grupo empresarial valora y por lo tanto desea proteger.

Se puede considerar como un activo de información a:

- ✓ Los datos creados o utilizados por un proceso del grupo empresarial en medio digital, en papel o en otros medios.
- ✓ El hardware y el software utilizado para el procesamiento, transporte o almacenamiento de información.
- ✓ Los servicios utilizados para la transmisión, recepción y control de la información.
- ✓ Las herramientas o utilidades para el desarrollo y soporte de los sistemas de información.
- ✓ Personas que manejen datos, o un conocimiento específico muy importante para el grupo empresarial (Por ejemplo: secretos industriales, manejo de información crítica, know how).

- **Programa no autorizado:**

Software que no cuenta con la aprobación del oficial de seguridad de la información para ser instalado en los equipos de cómputo del grupo empresarial o habiendo sido aprobado no cuenta con un licenciamiento vigente.

- **Propietario o Dueño**:

Es el individuo o grupo de individuos responsable de un activo de información. Son responsables de clasificar sus activos de información de acuerdo con el grado de sensibilidad y criticidad de estos, de documentar y mantener actualizada la clasificación efectuada, de definir qué usuarios podrán tener permisos de acceso a los activos de acuerdo con sus funciones y competencia, y de gestionar los riesgos[1] asociados a sus activos de información. Para el caso del grupo empresarial el propietario o dueño del activo de información corresponde al líder del proceso.

- **Información sensible:**

Se refiere a toda la información confidencial o reservada. La información sensible es toda aquella información importante para el negocio, que debe ser vigilada, controlada, no es de conocimiento púbico y adicionalmente puede estar restringido su acceso al interior del grupo empresarial.

DIRECTRIZ GENERAL

El líder de cada proceso identifica los activos de información asociados a cada sistema de procesamiento de la información en su respectivo proceso, con sus responsables y su ubicación, para luego elaborar un inventario con dicha información.

Así mismo, en el inventario se identifica, documenta y actualiza cualquier modificación de la información y de los activos asociados con los medios de procesamiento. Este es revisado con una periodicidad no mayor a un (1) año.

El uso de los activos de información pertenecientes al grupo empresarial es responsabilidad del propietario asignado; es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información.

1. INVENTARIO Y PROPIEDAD DE LOS ACTIVOS DE INFORMACIÓN

Los activos de información son identificados y controlados para asegurar su ubicación y evitar el uso inadecuado de los mismos.-

Los controles para los documentos digitales o electrónicos deben ser establecidos por el propietario de la información de acuerdo con la evaluación dada del activo de la información, declarada en la matriz de activos de información del área. Definir la pertinencia de ejecución de los controles acorde a la operatividad y uso del activo de información, para esto, el dueño evaluara la ejecución de los siguientes controles:

- Gestión de Acceso restringido: El propietario debe definir los usuarios que deben visualizar, modificar, ejecutar, eliminar o descargar una copia.
- Gestión de Copia de seguridad especial para el activo de información: El líder del proceso debe solicitar a la Dirección de Producción e infraestructura una gestión de copias de respaldo especial acorde a la necesidad del área solicitante y de acuerdo con la tecnología disponible por la organización.
- Gestión de versiones: El Dueño de activo de la información deberá definir el control de versiones y la cantidad de estos que se debe resguardar en copia de respaldo y si la necesidad es puntual al estándar establecido por la Dirección de Producción e Infraestructura deberá solicitarlos a través de mesa de ayuda y este sujeto a la capacidad tecnológica de la
- Manejo de clave para configuración: Se podrá designar claves a los archivos que necesite el dueño del activo de la información el cual será el único responsable de su uso y resguardo de la contraseña.
- Manejo de clave para su uso: Se podrá designar claves a los archivos que necesite el dueño del activo, para que visualicen y gestiones el activo de información y designara a quien considere este acceso, el cual será el único responsable de su uso y resguardo de la contraseña-

Todo activo comprado o adquirido en comodato por el grupo empresarial debe ser registrado y se le asigna un propietario o responsable.

El propietario de un activo designado por el grupo empresarial tiene la responsabilidad de mantener, asegurar el buen uso, clasificar y darle la protección adecuada.

Los activos deben ser valorados y clasificados con el fin de que se establezcan controles que sean adecuados para su protección.

Toda adquisición tecnológica del grupo empresarial es previamente evaluada en cuanto a requerimientos técnicos y de seguridad necesarios.

El proceso de gestión financiera y administrativa es el responsable de mantener actualizado el inventario de equipos y presentar un inventario de activos con fecha de compra y depreciación a la fecha, para la baja de los activos por obsolescencia, daño o el motivo que corresponda de acuerdo con lo definido en el documento MANUAL PARA LA ADMINISTRACIÓN Y CONTROL DE ACTIVOS FIJOS.

La vicepresidencia de tecnología cuenta en todo momento con un inventario actualizado del software de propiedad de la empresa, el comprado a terceros o desarrollado internamente, el adquirido bajo licenciamiento, el entregado y el recibido en comodato. Las licencias se almacenan bajo los adecuados niveles de seguridad cuando aplique y serán registradas en un inventario. En el inventario se referencia el número de usuarios permitidos por licencia y la fecha de renovación de la licencia.

2. USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN

Las personas que hagan uso de los activos de información del grupo empresarial tienen la responsabilidad de actuar de acuerdo con las directrices de seguridad de la información, Código de Ética y Conducta, disposiciones legales y contractuales, y demás disposiciones que establezca el grupo empresarial.

El acceso a la información es otorgado con base en los principios de need to know (necesidad de saber), por lo tanto, la información se comparte con las personas que demuestren la necesidad de conocer la información.

Los activos de información que pertenecen al grupo empresarial están destinados para propósitos laborales y son utilizados para asuntos personales siempre y cuando se les dé un uso razonable y no se genere algún riesgo para el grupo empresarial incumplimiento de las disposiciones internas o regulatorias.

Los colaboradores usan los programas y equipos autorizados y proporcionados por el proceso de sistemas y tecnología para la ejecución de las labores para las cuales fueron contratados.

Está permitido el uso de dispositivos personales (celulares, tabletas, portátiles) para manejar información del grupo empresarial, para lo cual:

- Se requiere aprobación de la Vicepresidencia de Riesgos y cumplimiento respecto de los cargos o situaciones especiales autorizadas para utilizar dispositivos personales.
- Desde la Vicepresidencia de Riesgos y cumplimiento se establecen los controles de seguridad de la información que se consideran adecuados para mitigar los riesgos asociados.

- El grupo empresarial tiene el derecho de monitorear y preservar cualquier comunicación que utilice la red del grupo empresarial, incluyendo datos, voz, logs, acceso a Internet y tráfico en la red para determinar el uso apropiado de los activos de información del grupo empresarial y el cumplimiento de las políticas y directrices de seguridad de la información y ciberseguridad.
- A la terminación de la relación laboral, se desinstala el software del grupo empresarial y se retira la información de su propiedad.
- En caso de pérdida, hurto, robo o acceso no autorizado al equipo personal que suponga riesgo para la información del grupo empresarial, el colaborador debe reportar de inmediato al oficial de seguridad de la información esta situación para tomar las medidas de protección de la información que este considere adecuadas.
- Para estos fines, el colaborador autoriza expresamente al grupo empresarial para instalar en su dispositivo personal el software que sea requerido para proteger la información corporativa y hacer buen uso de los sistemas de información del grupo empresarial.
- Los logs o archivos de auditoría de los activos de información críticos y/o que soportan la operación de la organización, deberán tener los controles necesarios para que no permitan modificar, eliminar y deberán ser resguardados según la necesidad de la operación.
- Los logs o archivos de auditoría de los activos de información críticos y/o que soportan la operación de la organización.

Mínimo una vez al año, la Vicepresidencia de Riesgos y cumplimiento realiza la revisión de los programas informáticos instalados en cada área. La descarga, instalación o uso de programas no autorizados se considera una violación a la Política de Seguridad de la Información del grupo empresarial.

3. DEVOLUCIÓN DE ACTIVOS

Los colaboradores del grupo empresarial realizan la devolución de todos los activos físicos y/o electrónicos asignados por el grupo empresarial en el proceso de desvinculación, de igual manera se documenta y entrega a quien se asigne para este fin, la información importante que posee de la labor que desempeñaron.

4. CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información del grupo empresarial o información propiedad de terceros a la cual tenga acceso el grupo empresarial, es clasificada para su uso. Para lo cual se han establecido los siguientes niveles de clasificación:

a. **P: Publica:** Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera del grupo empresarial, sin que esto implique un incumplimiento regulatorio, interrupciones en la operación, o afecte la confianza de los inversionistas.

b. **R: Reservada:** Información disponible para todos los procesos del grupo empresarial y que en caso de ser conocida por terceros sin autorización puede conllevar a sanciones o pérdidas económicas, interrupciones menores en la operación, y daño marginal en la relación con los inversionistas. Esta información no puede ser conocida por personas dentro y fuera del grupo empresarial sin autorización del propietario.

c. **C: Confidencial:** Información disponible sólo para un grupo limitado de personas del grupo empresarial, y que en caso de ser conocida por personas dentro o fuera del grupo empresarial sin autorización, puede conllevar sanciones significativas por parte de las autoridades competentes o litigios que afecten la reputación. Así mismo podría causar pérdidas económicas, interrupciones prolongadas en la operación y/o afectar drásticamente la confianza de los inversionistas

Para todos los tipos de información el líder de cada proceso es el responsable de establecer apropiadamente el nivel de sensibilidad de la información.

Información con múltiple clasificación de sensibilidad en un solo sistema: Cuando se consolida información con varias clasificaciones de sensibilidad, los controles usados deben proteger la información más sensible y la información se debe clasificar con el máximo nivel de restricción que contenga la misma.

5. ETIQUETADO DE LA INFORMACIÓN

Todos los casos en los cuales se exhibe en una pantalla o son presentados de otro modo por medio de un computador, información confidencial o reservada se indica que tipo de información es compartida.

6. GESTIÓN DE MEDIOS REMOVIBLES

Es restringido el uso de dispositivos de almacenamiento externo que no sean activos del grupo empresarial, tales como dispositivos móviles USB, Unidades quemadoras de CD y DVD.

De ser necesario el uso de dispositivo de almacenamiento externo, se solicita la autorización a la Vicepresidencia de riesgos y cumplimiento - Seguridad de la información a través del respectivo Líder de cada proceso, quien asume la responsabilidad de su custodia y buen uso.

En caso de que les sea autorizado, todos los colaboradores, pasantes, personal temporal, contratistas, funcionarios de los entes de control y miembros de las sociedades comisionistas, deberán tomar las medidas de precaución necesarias para el porte y transporte de información del grupo empresarial en medios magnéticos.

Toda información que durante su tratamiento permanezca en un dispositivo de almacenamiento externo, cuenta con la debida protección para evitar el acceso no autorizado.

Todos los proveedores de transporte de medios son fiables y de confianza y se realiza un proceso de selección para su contratación, que incluya requisitos de seguridad de la información.

7. CORREO ELECTRÓNICO

El sistema de correo electrónico y aplicativos asociados a la entidad son usados únicamente para el ejercicio de las funciones de competencia de cada colaborador y de las actividades contratadas en

el caso de los pasantes y personal temporal, incluyendo los funcionarios de los órganos de control y solo mientras se encuentren en comisión de visita dentro del grupo empresarial.

Los correos electrónicos de todo colaborador vinculado a la Bolsa Mercantil son gestionados bajo el dominio “bolsamercantil.com.co”. El grupo empresarial asigna a cada usuario una cuenta de correo electrónico, reservando el uso de accesos de acuerdo con las actividades del colaborador.

El uso del servicio de correo por parte del colaborador conlleva que éste acepta los términos de uso, las políticas de privacidad y las políticas particulares de uso publicadas por el grupo empresarial.

No está permitido distribuir mensajes con contenidos impropios y/o lesivos a la moral o de contenido ilícito o que atenten contra la dignidad e integridad humana, entre otros.

No está autorizado acceder a enlaces insertados en correos electrónicos que no provengan de un remitente de confianza.

No se pueden abrir correos electrónicos sospechosos y es obligación de cada usuario reportarlos a la Vicepresidencia de riesgos y cumplimiento, de manera inmediata a su detección.

No está autorizado participar en la propagación de cartas o correos encadenados, esquemas piramidales o similares.

No está permitido enviar correos con datos corporativos sensibles sin que exista una justificación asociada al cumplimiento de las funciones del colaborador, al cumplimiento de una obligación legal o contractual o una autorización dada por el dueño del activo de información.

Todos los usuarios están obligados a mantener en secreto las contraseñas de acceso para que su cuenta de correo no pueda ser utilizada por otras personas.

Estará prohibido a los usuarios usar cuentas de correo electrónico asignadas a otros colaboradores y el desvío de sus cuentas de correo electrónico.

En el servicio de correo se dispone de un mecanismo que permita filtrar y controlar el spam de correo, así como el flujo de correo entrante y saliente desde la óptica de virus.

En los eventos en que sea necesario mantener un mensaje en forma permanente, éste se almacena mediante un mecanismo que permita su consulta en cualquier momento.

Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

El grupo empresarial se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico asociado al grupo empresarial para cualquier propósito.

8. SERVICIO DE MENSAJERIA INSTANTANEA Y SERVICIO TELEFÓNICO

Todos los usuarios garantizan el uso correcto del servicio telefónico y de mensajería instantánea que tenga definido el grupo empresarial para este fin, como herramienta de trabajo.

El uso de los servicios de comunicación por parte de los usuarios conlleva la aceptación por parte de estos de:

• Ser sujetos de monitoreo de las conversaciones.
• Ser conocedores de la prohibición de transmitir información reservada o confidencial sin la debida autorización.
• Que el uso de los recursos es para el desempeño de su función y no para propósitos personales.

9. INTERNET

Los colaboradores, pasantes y personal temporal, así como los funcionarios de los órganos de control externo que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, aceptan, respetan y aplican las políticas y prácticas de uso de la red corporativa.

Todos los accesos a Internet se realizan a través de los canales de acceso provistos por el grupo empresarial; en caso de ser necesaria una conexión a Internet especial, ésta es notificada, aprobada por el director encargado y revisada y autorizada por la Vicepresidencia de riesgos y cumplimiento.

No se autoriza instalar programas para ver vídeos, televisión, escuchar emisoras o música vía Internet, en caso de que algún colaborador, lo requiera para desempeñar sus funciones, el director/Gerente remite la solicitud, debidamente justificada a la Vicepresidencia de riesgos y cumplimiento por medio del aplicativo de Soporte, quien, de considerarlo procedente, da el visto bueno para ejecutar la solicitud.

No se autoriza descargar aplicativos, programas o actualizaciones de internet; en caso de que algún colaborador, para desarrollar su actividad laboral, requiera descargar alguno de tales elementos, el director/gerente remite la solicitud a través de mesa de ayuda, debidamente justificada a la vicepresidencia de tecnología y con la aprobación del oficial de seguridad de la información.

En ningún caso se puede recibir ni compartir información en archivos adjuntos de dudosa procedencia en correos personales o corporativos para evitar el ingreso de virus al equipo.

El uso del servicio de navegación en Internet por parte de los usuarios conlleva la aceptación por parte de éstos de:

- Ser sujetos de monitoreo de las actividades que realicen en Internet.
- Ser conocedores de la prohibición de acceso a páginas no autorizadas.
- Ser conocedores de la prohibición de transmitir o almacenar archivos reservados o confidenciales del grupo empresarial que no les hayan sido autorizados.
- Ser conocedores de la prohibición de descargar software no autorizado.

10. HARDWARE

Se espera que los colaboradores protejan los equipos utilizados para acceder a la información del grupo empresarial frente a pérdida, daño o hurto.

En ningún caso se permite destapar o retirar la tapa de los equipos por personal diferente a la vicepresidencia de tecnología, salvo que cuente con la autorización previa y expresa de esta área.

Todo colaborador está obligado a informar oportunamente a la vicepresidencia de tecnología la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, recurso humano, o cualquiera otra, que altere la correcta funcionalidad del hardware en general. El reporte de las novedades se efectúa tan pronto se presente el problema por medio del aplicativo de Soporte.

Ningún colaborador podrá formatear los discos duros de los computadores excepto el personal autorizado por la vicepresidencia de tecnología.

Uso de equipos de trabajo

Todo portátil, laptop, notebook y demás equipos de cómputo que contengan información del grupo empresarial debe:

- Estar protegido mediante una contraseña.
- Protegerse en todo momento, evitando dejarlos desatendidos en áreas públicas.
- Tener instalado el antivirus licenciado por el grupo empresarial.

Cuando el colaborador viaje con dispositivos móviles que contengan información del grupo empresarial debe:

- Llevar sus dispositivos móviles como equipaje de mano. Estos elementos jamás pueden transportarse en la bodega.
- Cerrar la sesión y apagar su computador portátil, no utilizar las funciones “suspender” o “hibernar”.
- Reportar en caso de pérdida del dispositivo de manera inmediata.
- Evitar el uso del dispositivo en zonas en las que personas ajenas al grupo empresarial puedan leer fácilmente la información (ej.: salas de espera, sillas de aviones, entre otras).
- Dar un uso cuidadoso al dispositivo evitando daños físicos.

11. MANTENIMIENTO DE EQUIPOS

La reparación técnica de los equipos que sean activos del grupo empresarial o que estén en leasing o arriendo, que implique la apertura de estos, únicamente se realizan por colaboradores de la vicepresidencia de tecnología o el proveedor autorizado por dicha área.

Se realiza mantenimiento preventivo una vez al año a los equipos según las recomendaciones dadas por el fabricante o proveedor.

El mantenimiento es realizado por personal capacitado y autorizado por la vicepresidencia de tecnología para tal fin.

La vicepresidencia de tecnología tiene un cronograma de mantenimientos preventivos para los equipos del grupo empresarial.

Se registra la realización del mantenimiento, al igual que las fallas que impliquen mantenimientos correctivos.

Si el mantenimiento lo realiza un tercero se debe firmar un acuerdo de confidencialidad para proteger la información que contenga el equipo y el área responsable brinda el acompañamiento durante el mantenimiento y registrar las actividades realizadas.

Sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se asegura que se realicen mantenimientos periódicos con el fin de que dichos activos no se vean afectados por obsolescencia y se asegura la disponibilidad e integridad de los equipos de manera permanente. Por lo tanto, se revisa constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes. Esta labor se realiza por los ingenieros de soporte de la vicepresidencia de tecnología o por quien esta designe.

La vicepresidencia de tecnología mantiene un inventario actualizado de los equipos existentes en el grupo empresarial.

ANEXO No. 7 – POLÍTICA INTERNA DE LAS OPERACIONES Y COMUNICACIONES

ALCANCE

El alcance de la presente directriz de seguridad de la información se extiende a todos los sistemas de información utilizados en las diferentes áreas de la organización.

La información contenida en el presente documento es de aplicación exclusiva para la Bolsa o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

RESPONSABILIDADES

La vicepresidencia de tecnología garantizará las condiciones tecnológicas para la ejecución de la presente política.

DIRECTRIZ GENERAL

Los procedimientos y responsabilidades de operación y administración de la plataforma tecnológica y de seguridad de la organización, están documentados, garantizando un adecuado control de cambios y un manejo eficiente de incidentes de seguridad de la información en la organización.

Los activos de información se administran y operan con la respectiva segregación de funciones. El valor del activo es establecido por el responsable para disminuir la exposición a riesgos de seguridad de la información y aseguran que la planificación y puesta en producción de los sistemas de información tienen en cuenta los requerimientos de seguridad de la información.

1. GESTIÓN DE CAMBIOS

La vicepresidencia de tecnología define procedimientos para el control de los cambios significativos en el ambiente de pruebas, pre-producción y producción. Estos cambios son evaluados previamente en aspectos técnicos, de seguridad de la información y ciberseguridad (en los cambios que aplique).

El procedimiento de control de cambios requiere como mínimo que los cambios:

- Esten justificados y debidamente sustentados
- Esten convenientemente registrados, clasificados y documentados
- Han sido cuidadosamente probados en un ambiente de prueba
- No afecten de manera significativa la calidad de los servicios de TI
- Se reflejen en la base de datos de componentes (activos de TI)
- Están acompañados de un plan para deshacer el cambio – Rollback- en caso de que el cambio pueda generar problemas en el servicio por cualquier falla que pueda presentar.
- Asegurar que en la instalación de un cambio participe todo el personal de soporte y usuarios necesarios para lograr una implementación exitosa.

Todo cambio significativo sobre la infraestructura o servicios de TI, sigue lo definido en el procedimiento de control de cambios.

Todo cambio significativo en la plataforma tecnológica queda formalmente documentado desde su solicitud hasta su implementación. Este mecanismo provee herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio significativo en los sistemas de información, sean sistemas nuevos, modificaciones, actualizaciones y nuevas versiones solamente son ejecutados, cumpliendo los requerimientos establecidos en el procedimiento de Manual de Gestión de Proyectos y Cambios, definido por la vicepresidencia de tecnología. Las pruebas mínimas para garantizar la integridad de la información en producción son: planeadas, ejecutadas, documentadas y controlados sus resultados. Las pruebas son previamente establecidas y el ambiente de pruebas o preproducción es el más parecido en su configuración al ambiente real de producción.

Los cambios significativos reflejan los detalles de las actividades previas, las actividades durante el cambio, las actividades posteriores al cambio y las actividades en caso de regreso del cambio (rollback).

Todo cambio significativo a un recurso informático de la plataforma tecnológica relacionado con mantenimiento de software o modificación de parámetros se realiza de tal forma que no disminuya la seguridad existente a menos que se realice un análisis de aceptación de riesgo que habilite el

cambio. Antes de que un nuevo sistema sea adquirido, se especifican claramente los requerimientos importantes de seguridad de la información.

Los cambios que puedan generar afectación de los servicios o la operación del grupo empresarial se realizan por medio de ventanas programadas en horarios fuera de operación y estas son aprobadas por el área de tecnología y las áreas de la organización que puedan tener algún tipo de impacto generado por el cambio.

Previo a la utilización de un nuevo servicio de procesamiento de información en la organización, realiza un ambiente de prueba, para garantizar que el cambio no afecte la seguridad de la información existente. Las pruebas sobre el software a adquirir contemplan aspectos funcionales, de seguridad y técnicos; así como, una verificación a la documentación mínima requerida y la revisión de los procesos de retorno a la versión anterior.

Antes de implementar un software en producción se recibe la confirmación de parte del usuario líder que se ha realizado la divulgación de la documentación de entrenamiento, operación y de seguridad adecuados, la capacitación al personal involucrado, licenciamiento requerido y los ajustes de parámetros en el ambiente de producción.

Cualquier cambio significativo que se requiera realizar en los equipos de cómputo de la organización (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y los directores de la vicepresidencia de tecnología encargados tomarán autónomamente la decisión.

Los cambios significativos están aprobados por la vicepresidencia de tecnología o los directores de TI encargados del respectivo cambio y las áreas de la organización involucradas o que puedan tener algún tipo de impacto por el cambio.

Los siguientes cambios significativos deben tener la aprobación del oficial de seguridad de la información:

- Cambio de política de contraseña en aplicaciones o sistemas de información.
- Creación, modificación o eliminación de reglas de firewall o grupos de seguridad en AWS.
- Creación, modificación o eliminación de servicios de seguridad en nube o en la oficina Teleport.
- Modificación de los niveles de cifrado en aplicaciones y sistemas de información.
- Cambios en las líneas base de configuración de las instancias y/o servicios de AWS.
- Creación, modificación o eliminación de las reglas del WAF (firewall de aplicaciones)
- Creación, modificación o eliminación registros de auditorías de aplicaciones, sistemas de información y servicios de seguridad de la información y ciberseguridad.
- Creación, modificación o eliminación de los servicios de seguridad de Office 365 y herramientas de control antimalware, control de navegación, conexión remota VPN.

2. GESTIÓN DE CAPACIDAD

Se controla la demanda de capacidad de los sistemas de información de la organización e igualmente se realizan proyecciones de los requerimientos de capacidad hacia el futuro para que sean suficientes y puedan satisfacer la demanda de almacenamiento de información.

Los recursos que soportan la operación deben ser controlados con el fin de que se tenga la capacidad adicional disponible y suficiente para cuando sea necesario utilizarla, de acuerdo con su tipo de licenciamiento y tecnología disponible a la necesidad de la operación:

- Servidores de dominio
- Servidores y servicio de AWS
- Servidores de aplicaciones
- Servidores de aplicaciones web
- Servidores de base de datos
- Canales de comunicación
- Servicio de correo electrónico
- Tercerización del servicio de Impresoras
- Estaciones de trabajo
- Servicios de Office 365
- Licenciamiento, dominios y certificados digitales

Se mantiene actualizado el software de la organización y realizar una adecuada gestión de parches sobre el mismo.

3. SEPARACIÓN DE AMBIENTES

Los ambientes de desarrollo, prueba, pre-producción y producción de los sistemas de información de la organización están separados, para garantizar la seguridad en cada ambiente y prevenir los riesgos generados por cambios accidentales o el acceso no autorizado.

Se actualiza la documentación y los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio en la organización.

Los ambientes de desarrollo y prueba están separados por controles adecuados y cumplir con los siguientes requisitos:

- Las pruebas de servicios de procesamiento de información se realizan en ambientes de prueba independientes a los de producción.
- Se emplean diferentes nombres de usuario y/o contraseñas de usuario.
- Los ambientes de prueba o preproducción son los más parecidos a los ambientes de producción.
- El software se prueba en diferentes sistemas, equipos de computación y en diferentes dominios o directorios de acuerdo con el alcance definido y requisitos de operación.

- No se copian datos sensibles de la organización en ambientes de prueba o preproducción. En caso de que sea necesario usar datos de producción se deben aplicar controles compensatorios que mitiguen riesgos de fuga de información.
- Los ambientes de prueba o preproducción tienen acceso restringido y debidamente autorizado.

4. PROTECCIÓN CONTRA CÓDIGO MALICIOSO

No se pueden instalar en los equipos asignados al personal del grupo empresarial hardware ni software sin previa autorización de la vicepresidencia de tecnología.

No se descargan ni actualizan programas desde Internet en los equipos de la organización, salvo las actualizaciones autorizadas por la vicepresidencia de tecnología teniendo en cuenta las necesidades de la organización.

En cualquier caso y como control mínimo, las estaciones de trabajo de todo el personal de la organización están protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus.

La ejecución del antivirus desde el administrador debe estar programado para que examine cada computador de la red como mínimo diariamente con base en los análisis de riesgo.

Cuando se detecte un virus en la red de la organización, la vicepresidencia de tecnología emprende de inmediato brigadas de limpieza de virus.

Los usuarios tienen prohibido almacenar archivos personales en su estación de trabajo o en las unidades compartidas. En estos casos el grupo empresarial no podrá garantizar ningún tipo de reserva sobre esta información.

La vicepresidencia de tecnología es la responsable del mantenimiento, actualización, configuración y licenciamiento del software anti-virus de la organización.

5. ADMINISTRACIÓN Y USO DEL ANTIVIRUS

El grupo empresarial posee un esquema de protección antivirus centralizado que realizará la labor de protección a el grupo empresarial . Las características que tienen son las siguientes:

- Análisis de spyware y malware en el momento del acceso.
- Protección para las imágenes virtuales fuera de línea.
- Protección contra amenazas de día cero.
- Prevención de intrusos.
- Reglas de protección de acceso.
- Una única consola de gestión.
- Verificación de autenticidad de los sitios.
- Análisis de correo electrónico que se administra desde la misma suite de correo.

Esta herramienta está configurada de tal forma que permita: realizar la instalación remota para clientes nuevos que se encuentren conectados al dominio, programar tareas de escaneo de virus en los equipos, así como también generar políticas de protección hacia los clientes vinculados en el servidor. En los clientes se instalará un agente que cumpla las funciones de antivirus y antispyware, el cual generará protección contra los riesgos de virus, software espía, protección automática del sistema, Scan-Engine, etc.

La herramienta verificará y descargará actualizaciones de la base de datos de virus con una periodicidad como mínimo diariamente, permitiendo contar con alta protección ante nuevos ataques de virus.

6. CÓDIGOS MÓVILES

Está prohibido escribir, generar, recopilar, difundir, copiar, ejecutar o intentar introducir cualquier código de computadora diseñado para auto-replicarse, dañar o entorpecer el acceso a cualquier equipo de la organización, red o información.

La ejecución de códigos móviles autorizados por el proceso de sistemas y tecnología, únicamente se pueden realizar con aislamiento lógico.

Está prohibido el uso y recepción de códigos móviles diferentes a los aprobados por la vicepresidencia de tecnología.

7. RESPALDO Y RETENCIÓN

Es responsabilidad de los administradores de los sistemas, identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su criticidad.

Las copias de seguridad son una forma de protección de datos la cual permite la recuperación de la información, sean datos, bases de datos, aplicaciones, entre otros, en el caso de que tenga lugar perdida o falla del Software o Hardware, debido a desastres naturales, procedimientos administrativos, fallos de disco, ciberataques, entre otros.

El propósito de estas directrices es establecer las condiciones de acceso, administración uso, control y seguridad de las copias de seguridad de la información de la Infraestructura de la organización, la ejecución de las copias de seguridad debe ser cumplidas estrictamente por parte de los administradores de la infraestructura de la organización con el propósito de salvaguardar la información en caso de fallas para ello, se dan los siguientes tipos de copia según las necesidades.

Tipos de copias de seguridad:

- Copia Total: Este tipo de Copia hace un respaldo completo de todos archivos del recurso o carpeta de datos.
- Copia de seguridad diferencial: únicamente contiene los archivos que han cambiado desde la última vez que se hizo la copia. Por lo tanto, se incluyen sólo los archivos nuevos y/o modificados.

- Copia de seguridad incremental: Este tipo de copia se hace un respaldo de todos los archivos que han sido modificados
-

La política de copias de seguridad de la información su actuar se basa en el **instructivo para la gestión de backups versión 3** donde se define:

- Respaldo de información ofimático (Correo Electrónico, SharePoint, OneDrive, Teams, Planner).
- Respaldo de Instancias (Máquinas virtuales).
- Gestión de Backups de base de datos.
- Restauración, Retención y monitoreo.

Toda información sensible de acuerdo con la clasificación establecida por el grupo empresarial tiene un proceso periódico de respaldo, un periodo de retención determinado, la fecha de la última modificación y la fecha en que deja de ser sensible o se degrada; sin embargo, la información no se guarda indefinidamente por lo cual se determina un periodo máximo de retención para el caso en que no se haya especificado este tiempo.

La información sensible (confidencial o reservada) tiene un respaldo, copias recientes completas en sitio externo a la entidad o en un lugar lejano de donde reside la información origen; en caso de que no se tengan copias de la información crítica no se llevan a cabo procesos de restauración puesto que se corre el riesgo de perder la única copia que se tenga.

Es responsabilidad de los colaboradores del grupo empresarial almacenar la información sensible de la organización que utilicen para sus actividades diarias en la carpeta de OneDrive y/o SharePoint, esto con el fin de garantizar el respaldo de esta información. Todos los documentos, archivos y/o carpetas que se encuentren fuera de OneDrive quedará sin copia de respaldo.

La vicepresidencia de tecnología cuenta con mecanismos de backups que permita administrar, programar y ejecutar tareas de respaldo automático.

Toda la información confidencial o reservada de la organización ya sea que pertenezca a la matriz de activos de información o que sea de interés para un proceso operativo o de misión crítica se respaldada por copias de seguridad. Todos los propietarios de información son responsables de esta actividad con el acompañamiento de la vicepresidencia de tecnología.

Previo a la entrada en producción de un sistema de información (activo de información) se tienen documentados procedimientos de respaldo y recuperación.

Todos los procedimientos de respaldo generan un registro que permita la revisión del resultado de la ejecución y dentro de lo posible, se realizarán con la opción de verificación de integridad.

Los sitios donde se almacenan las copias de respaldo están física o lógicamente seguros, con los controles físicos y ambientales según las normas estándares.

La vicepresidencia de tecnología realiza pruebas controladas de los backups para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Las copias de seguridad de información sensible son ejecutadas de acuerdo con cronogramas definidos por la dirección de tecnología.

La vicepresidencia de tecnología establecerá controles para evitar que en los servidores/Instancias de almacenamiento se almacene información de tipo no misional como por ejemplo fotos, música o videos a menos que el área usuaria lo requiera para el desarrollo de sus funciones.

Pruebas de recuperación de copias de respaldo: se efectúan pruebas de recuperación de las copias de respaldo semestralmente. Estás pruebas servirán para constatar que se puedan obtener correctamente los datos grabados, con el fin de garantizar su disponibilidad al momento de ser requeridos.

Las pruebas se formalizan en el formato definido para este fin y el soporte correspondiente de la persona que la realizó.

Cifrado de copias de seguridad, con el fin de evitar que se revele o utilice información sensible, valiosa o crítica de la organización, por parte de terceros no autorizados, la información almacenada en AWS y registrada en medios informáticos de back up están en forma cifrada.

Registro y seguimiento: Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica, se efectuará un seguimiento a los accesos realizados por los usuarios a la información del grupo empresarial, con el objeto de minimizar el riesgo de pérdida de integridad y/o confidencialidad de la información.

Los sistemas de procesamiento de información y redes de la organización considerados críticos son monitoreados para garantizar la detección de incidentes de seguridad en lo posible cercano a tiempo real y la identificación de fallas en los sistemas.

Los registros de auditoría se conservan durante mínimo de 60 días. Esto aplica siempre y cuando la aplicación o servicio permita la consulta de estos registros. Los registros de auditoría de usuario deben contener la siguiente información:

- Identidad del sistema
- ID de usuario
- Inicio de sesión éxito / fallidas
- Éxito de cierre de sesión / sin éxito
- Acceso a las aplicaciones no autorizadas
- Los cambios en las configuraciones del sistema
- El uso de cuentas privilegiadas (por ejemplo, gestión de cuentas, cambios de políticas, configuración de dispositivos)
- Violaciones a políticas
- Errores del sistema (fecha y hora)

Se protege el acceso a los registros de auditoría para evitar que accesos no autorizados los modifiquen o eliminen.

El personal operativo y los administradores del sistema deben mantener un registro de sus actividades.

8. SINCRONIZACIÓN DE RELOJES

La vicepresidencia de tecnología implementa la sincronización de relojes de los sistemas de información a un único servidor NTP (Network Time Protocol – protocolo de tiempo en la red).

9. CONTROL DE SOFTWARE OPERACIONAL

Todo Software que se utilice en el grupo empresarial, es adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos definidos por la vicepresidencia de tecnología para este fin. Adicionalmente, se tiene configurado desde el directorio activo, una política que no permita instalación de software a ningún usuario, excepto los administradores.

Previo a la adquisición, compra o instalación de cualquier software no ofimático, se debe de tener la aprobación de la Vicepresidencia de riesgos y cumplimiento por medio del oficial de Seguridad de la Información o autorizador para tal fin.

Todo Software instalado es consecuente con el inventario de las licencias adquiridas para llevar una adecuada administración y control de estas.

Los profesionales encargados de realizar la instalación o distribución de software sólo instalarán productos con licencia y software autorizado.

Semestralmente la Vicepresidencia de riesgos y cumplimiento realizará la revisión de los programas utilizados en cada proceso.

La descarga, instalación o uso de aplicativos o programas informáticos no autorizados es considera como una violación a las Políticas de Seguridad de la Información y ciberseguridad del grupo empresarial.

No se autoriza descargar aplicativos, programas, actualizaciones o archivos de internet por personal no autorizado.

Está prohibido actualizar el software de sistemas críticos de la organización de forma automática, ya que pueden afectar la operación y continuidad de las operaciones.

Se encuentra prohibido el uso e instalación de juegos en los computadores de la organización.

10. GESTIÓN DE VULNERABILIDADES TÉCNICAS

El Equipo de Seguridad de la Información basado en el inventario de activos de la Vicepresidencia de Tecnología, definirá los activos objeto de la verificación que se consideren críticos (internos y externos) y soporten la operación de la , estos deberán ser presentado junto con el cronograma de ejecución ante el Grupo de Gestión de Vulnerabilidades, quien deben aprobar los ciclos de análisis de vulnerabilidades, planes de acción propuestos por los administradores de la plataforma, re-test y cierre de ciclos de vulnerabilidades.

La Identificación de hallazgos debe ser con software licenciado el cual debe homologar las vulnerabilidades por el CVE (Common Vulnerabilities and Exposures).

El alcance de las pruebas de análisis de vulnerabilidades solo contempla dispositivos tecnológicos pertenecientes a la organización, los dispositivos tecnológicos de proveedores, clientes o cualquier proyecto contemplado se registrará como escaneo de vulnerabilidades a demanda y deberá exponerse su resultado y planes de acción ante el Grupo de Gestión de vulnerabilidades.

Es responsabilidad del administrador de la plataforma tecnológica y de las aplicaciones supervisar, ejecutar y controlar las acciones pertinentes para mitigar los riesgos ocasionados por las amenazas detectadas en las pruebas de análisis de vulnerabilidades, según la criticidad de estas.

Los miembros del grupo de gestión de vulnerabilidades se encuentran definido en el “PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES".

Ciclo del análisis de vulnerabilidades

Definir el alcance: Identificar y priorizar los activos de información del Core del negocio de acuerdo con el análisis y necesidad del negocio, este debe ser aprobado por Grupo de Gestión de Vulnerabilidades.

Evaluación de Vulnerabilidades: Se debe ejecución de escaneo en la infraestructura de la organización definidos y aprobados por el Grupo de Gestión de Vulnerabilidades, este análisis deberá ser ejecutado con la herramienta aprobada y dispuesta para la prueba.

Gestión de Remediación: Diseñará y ejecutará planes de acción para remediar las vulnerabilidades descubiertas, mediante un registro y seguimiento a planes de acción, por parte de los administradores de la plataforma y del administrador del activo de información analizado.

Re-Test de Validación: EL equipo de seguridad de la Información ejecutará nuevamente escaneos luego de ejecutar el plan de remediaciones o después de cualquier cambio representativo a los activos de información.

Informe: Se debe documentar la gestión de cada ciclo de evaluación de vulnerabilidades el cual se le presentará ante el comité de Riesgos como evidencias de las remediaciones para las auditorías de gestión.

Remediación de vulnerabilidades

Los niveles de impacto de las vulnerabilidades identificadas en los análisis de vulnerabilidades y Hacking Ético se reportarán bajo estas definiciones, y se deberán realizar planes de acción de remediaciones para las vulnerabilidades de tipo Crítica, Alta y Media en los tiempos establecidos en esta política. Esta denominación debe coincidir con la clasificación de la herramienta de Escaneo de vulnerabilidades corporativa.

CRITICIDAD	DESCRIPCIÓN	MÁXIMO TIEMPO DE REMEDIACIÓN
Crítica	Se define critica debido se tiene la máxima exposición a que un ciber atacante puede obtener fácilmente el control total del dispositivo afectado, lo cual comprometer toda la infraestructura corporativa, este nivel de severidad contempla el acceso completo de lectura y acceso de escritura a los activos de información con posible ejecución remota de comandos y exposición a la presencia de puertas traseras (Backdoors), APTs (Amenazas Avanzadas Persistentes – Advanced Persistent Threats).	30 días
Alta	Se define como altas porque hay mayor probabilidad de intruso informático control del activo de información afectado, lo que puede generar fugas de información.	40 días
Media	Se definen media porque existe la posibilidad de acceder a información específica almacenada en el dispositivo afectado, incluyendo la configuración de seguridad. Las vulnerabilidades en este nivel pueden incluir la divulgación parcial del contenido de archivos, exploración de directorios, la divulgación de las reglas de filtrado y mecanismos de seguridad, ataques de denegación de servicio, y el uso no autorizado de los servicios, tales como-retransmisión de correo electrónico.	60 días
Bajas e Informativas	Se definen bajas por que puede tener o no la posibilidad de explotación, podría estar derivada de una vulnerabilidad mayor sin embargo se debe tener en cuenta la implementación de controles alternos para este tipo de exposición.	75 días

Ciclo del Hacking Ético

- **Fase de reconocimiento**

Escaneo de infraestructura: Identificación de equipos activos, bases de datos en los rangos internos/externos de del alcance de la prueba; en esta actividad se debe revisar que las segmentaciones de red estén configuradas correctamente.

Escaneos de activos de Información: descubrir puertos y servicios expuestos, identificación de entradas habilitadas para acceso sobre el dispositivo evaluado y los servicios prestados.

Enumeración de información: Identificación de banners (letreros o descripciones de servicios que informan la naturaleza y posible configuración de un servidor), cuentas de correo, usuarios, etc.

- **Fase de Ataque**

Identificación de vulnerabilidades: Validar las vulnerabilidades vigentes para cada servicio y plataforma teniendo en cuenta versiones de sistema operativo y actualizaciones, entre otros.

Explotación de vulnerabilidades sobre puertos y servicios habilitados: Ejecución de ataques controlados y orientados a vulnerar aquellas entradas identificadas. Esta actividad se realiza sobre vulnerabilidades que no afectan al servicio y que pueden explotarse sin causar fallas en el sistema; si no, se evaluará el impacto directamente con el cliente para programarlas en horarios o ventanas de tiempo específicos.

Elevación de privilegios: Búsqueda del control total del dispositivo evaluado (apoderamiento de la máquina), en los casos en donde sea posible.

- **Fase de Reporte**

Recopilación y entrega de evidencia: Se debe recopilar la evidencia de la intromisión de los objetivos y los pasos que se realizaron en el hacking Ético.

Generación y presentar del Informe: Se debe generar un informe con las falencias, posibles controles y lecciones aprendidas

Periodicidad de las pruebas

- **Escaneo de Vulnerabilidades**

Estos escaneos se ejecutan a los dispositivos ubicados en la red externa o interna como servidores, equipos de comunicación, aplicaciones web, dispositivos de la red, estaciones de trabajo, la periodicidad de ejecución de pruebas de vulnerabilidades será trimestral.

Para el informe trimestral de análisis de vulnerabilidades en que se realizó la solicitud se considerará todo análisis de vulnerabilidades a demanda a nuevos desarrollos, proyectos, actualizaciones y/o despliegues tecnológicos.

- **Hacking Ético**

Las pruebas de Hacking Ético deben ejecutarse como mínimo con una periodicidad anual y se deben planear teniendo en cuenta los proyectos. servidores, equipos de cómputo, redes, redes inalámbricas, y pruebas de ingeniería social.

11. GESTIÓN DE LA SEGURIDAD EN LAS REDES

Se tiene un inventario actualizado de los componentes de red de la organización sobre los cuales se deben identificar los riesgos de seguridad asociados y definir mecanismos para su adecuada gestión.

Toda conexión a la red del grupo empresarial tiene mecanismos de autenticación para verificar la validez del usuario que se conecta.

Todas las conexiones desde la red del grupo empresarial a redes externas deben estar protegidas por un firewall y se establecen reglas apropiadas para filtrar el tráfico permitido entre las mismas, de igual manera, se tienen mecanismos de seguridad perimetral.

La red de la organización es monitoreada para detectar prontamente fallas técnicas en la infraestructura.

La información sobre las direcciones lógicas internas, configuraciones e información de los sistemas de comunicación y cómputo del grupo empresarial, son de carácter confidencial al igual que la arquitectura y topología de red.

Las conexiones tanto internas como externas que tienen sistemas críticos conectados cuentan con un tiempo máximo de inactividad, transcurrido dicho periodo de tiempo la sesión es cerrada de forma automática.

La organización realiza al menos dos veces al año una prueba de vulnerabilidades técnicas asociadas a la infraestructura tecnológica.

11.1 CONTROL DE ACCESO A LA RED

La infraestructura del grupo empresarial está separada por Vlans (Virtual local área) para garantizar la confidencialidad de los datos que se transmitan de acuerdo con los análisis de riesgos.

11.2 GESTION DE NOMBRES DE DOMINIO

Con el fin de preservar externamente el buen nombre de los dominios que hace uso el grupo empresarial en el rango direcciones IP públicas, la vicepresidencia de tecnología mantienen un registro que almacene la siguiente información:

- El nombre, propósito y vigencia del dominio DNS albergado.
- Las direcciones IP/nombres de dominio correspondientes a los servidores DNS de ese dominio.
- Los datos de contacto del responsable administrativo del dominio.
- Los datos de contacto del responsable técnico del dominio.

Esta información de registro se mantiene en la entidad elegida por la organización donde se tenga el registro.

En ningún caso se permite crear registros DNS que, correspondiendo a un dominio albergado dentro del grupo empresarial, haga referencia a direcciones de red externas. La finalidad de esta medida es evitar que se puedan asumir como propios, contenidos ajenos a la entidad.

11.3 EN EL USO DE LA RED

Los principios que guían el buen uso de la red por parte de los colaboradores se derivan en primer lugar de la filosofía de utilización de las nuevas tecnologías del grupo empresarial y, en segundo lugar, en los derechos y obligaciones adquiridas como integrantes de la red de datos.

Las pautas de conducta que marca esta directiva de uso son conocidas y respetadas por cualquier persona que utilice la red del grupo empresarial, especialmente por aquellas que mantengan una relación contractual, con el objetivo de proteger los siguientes aspectos:

- El grupo empresarial utilizará correctamente los recursos tecnológicos como canales de internet y sistemas de información, de igual manera que facilitará el acceso a su infraestructura de red al personal autorizado y denegándolo a personas u organizaciones no autorizadas.

- Los recursos de red del grupo empresarial podrán ser utilizados para fines personales siempre y cuando se utilicen de manera razonable y ello no vaya en contra de disposiciones incluidas en el contrato de trabajo, en el reglamento interno de trabajo, en el código de ética y conducta y demás disposiciones internas del grupo empresarial que puedan aplicar.

- La Entidad podrá establecer los mecanismos para poder identificar en caso de incidente, los nodos o las personas que están actuando a través de la red.

12. ZONAS DE SEGURIDAD

Dentro de la red de comunicaciones del grupo empresarial, existirán varios entornos que comparten una misma infraestructura pero que, debido a los requerimientos de seguridad impuestos por su finalidad, se mantendrán separados, y el Internet Inalámbrico. La estructuración por zonas no guarda ninguna relación con la distribución física de estos nodos.

13. CONECTIVIDAD ENTRE ZONAS

La estructuración por zonas permite, entre otras funcionalidades, aplicar mecanismos que ayuden a hacer efectivos los objetivos de seguridad de cada entorno. Se establecen filtros de tráfico de red entre zonas, orientados a reducir el riesgo de que se produzca un incidente de seguridad.

Dentro de cada zona, si así se requiere, se podrán establecer filtros adicionales. En los casos en los que sea necesario extremar las medidas de seguridad, se limitará la conectividad a los nodos y servicios imprescindibles para la prestación del servicio.

14. ACCESO A INTERNET

El conjunto de restricciones de acceso a internet tendrá como fin limitar la cantidad de incidentes de seguridad que puedan ser originados de forma intencionada o accidental, por nodos pertenecientes a la red del grupo empresarial. Debido al cambio frecuente de las técnicas de ataque

en materia de seguridad informática, estas restricciones serán actualizadas en cada revisión de la directiva de seguridad en la red.

De esta manera se permitirá todo el tráfico saliente, excepto el relacionado con:

- Violence/Hate/Racism
- Intimate Apparel/Swimsuit
- Nudism
- Pornography
- Weapons
- Adult/Mature Content
- Cult/Occult
- Drugs/Illegal Drugs
- Illegal Skills/Questionable Skills
- Sex Education
- Gambling
- Alcohol/Tobacco
- Chat/Instant Messaging (IM)
- Games
- Usenet News Groups
- Religion
- Kid Friendly
- Internet Auctions
- Gay and Lesbian Issues
- Humor/Jokes
- Multimedia
- Pay to Surf Sites
- Abortion / Advocacy Groups
- Hacking/Proxy Avoidance Systems
- Web Communications
- Personal san Dating
- Society and Lifestyle
- Restaurants and Dining
- Sport / Recreation
- Vehicles
- Freeware / Software Download
- Social Networking
- Malware

Lo anterior, con el fin de cumplir la directiva relacionada con los criterios de la información aplicadas en el uso de la red anteriormente nombrada.

La vicepresidencia de tecnología asegura el bloqueo al acceso de páginas de contenido anteriormente mencionadas, hacking, descargas (FTP), y cualquier página que represente riesgo potencial para la organización mediante el uso de servidor proxy, firewall, software o herramienta que mejor se ajuste a la necesidad.

Las excepciones de acceso serán solicitadas por el gerente o director de cada área, según la necesidad del cargo y con el visto bueno del oficial de seguridad de la información.

15. PUBLICACIÓN DE SERVIDORES

Para la publicación hacia Internet de las aplicaciones instaladas en la entidad, se realizará bajo los respectivos protocolos http y https según sea el tipo de aplicación, con el fin de permitir el acceso a las personas externas por medio de Internet sólo por los puertos establecidos para dichas aplicaciones.

Para realizar estas publicaciones se utilizará el método de NAT (Network Address Translation), el cual es basado en el traslado de direcciones IP privadas de la red LAN, en direcciones públicas de la red WAN. Esto aplica para las redes de Teleport.

16. SEGURIDAD EN LOS SERVICIOS DE RED

La vicepresidencia de tecnología mantiene instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la organización.

De igual manera, controla el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la organización o utilizando los mecanismos provistos por el servicio de Cloud utilizado por la organización para este fin.

17. TRANSFERENCIA DE INFORMACIÓN

La información que es compartida es protegida de interceptación, copia, modificación y destrucción no autorizada.

Todo acuerdo de intercambio de información específica tipo de información intercambiada, clasificación de la información y los controles que aplica el receptor de la información para su protección.

La información confidencial que se envíe o entregue a los clientes por cualquier medio digital (correo electrónico, DVD, CD, USB, entre otros) contar con los controles que mitiguen el riesgo de fuga de información y el acceso no autorizado

La información confidencial que se envié a proveedores, cliente u otras terceras partes en documento físicos se envía en sobre cerrado y por medio de correo certificado.

Toda información que se transporte físicamente está debidamente identificada, marcada y clasificada, conforme a lo establecido por la organización.

Todo intercambio de información que realice vía correo electrónico cumple con lo establecido en la Directriz de Gestión de Activos de Información.

Toda información públicamente disponible tiene los controles necesarios para evitar que la misma sea modificada o eliminada de forma no autorizada.

18. RESTRICCIONES ESPECÍFICAS DE DIVULGACIÓN DE INFORMACIÓN

La información específica sobre las vulnerabilidades del sistema, como los detalles de una reciente brecha, no es divulgada a personas no autorizadas, está divulgación es estrictamente controlada.

Las políticas de seguridad de la información, las directivas y los procedimientos sólo pueden ser divulgados a los colaboradores del grupo empresarial y a ciertas partes externas (como auditores, revisoría fiscal, etc), que requieran la información.

19. TRABAJO REMOTO

En los casos que los colaboradores deban usar los equipos de procesamiento de datos fuera de las instalaciones del grupo empresarial, se deben cumplir los siguientes lineamientos:

Garantizar el cuidado del equipo en cuanto a los aspectos físicos de seguridad, transporte, condiciones óptimas de operación y conexión a redes seguras evitando la conexión a redes públicas.

Los dispositivos móviles asignados a los colaboradores del grupo empresarial son asegurados mediante pólizas que cubran los principales riesgos a los que están expuestos.

Estar conectados mínimo tres veces a la semana a la VPN para que los equipos se actualicen con las políticas definidas por la compañía.

ANEXO No. 8 – POLÍTICA INTERNA RELACION CON TERCEROS

ALCANCE

La información contenida en el presente documento es de aplicación exclusiva para la Bolsa o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

RESPONSABILIDADES

Directriz que aplica a los lideres de procesos que tienen a su cargo contratistas, proveedores de outsourcing, consultores y/o contratistas externos, personal temporal y en general a todos los usuarios de la información que realicen estas tareas para el grupo empresarial.

DIRECTRIZ GENERAL

La organización establece mecanismos de control en sus relaciones con terceras partes en la presente directriz y en los manuales de los procesos, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información del grupo empresarial.

Se establecen criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes de acuerdo con el Manual de Compras. Así mismo, respecto de aquellos proveedores que se consideren críticos desde la óptica de seguridad de la información, en el proceso de selección se realiza una evaluación de las políticas, prácticas y procedimientos de los proveedores para asegurar que cumplen con las necesidades del grupo empresarial en materia de integridad, confidencialidad y disponibilidad de la información, la cual es realizada por el oficial de seguridad de la información.

Los responsables de la realización y/o firma de contratos o convenios con terceras partes informan las políticas, normas y procedimientos de seguridad de la información, adicionalmente realizan el seguimiento, control, revisión y auditoría a los servicios suministrados por los proveedores y/o contratistas. La VP. Jurídica asegura que contractualmente se incluyan las cláusulas y anexos

correspondientes a las obligaciones en materia de seguridad de la información; en caso de contratos de adhesión que los mismos sean adecuados desde esta óptica.

Los servicios tercerizados se prestan de manera controlada, organizada y segura. Para aquellos contratos con terceros que supongan riesgos en materia de seguridad de la información, la organización generará un SLA (nivel de acuerdo de servicio) y requisitos de seguridad de la información, con los que cumplen las terceras partes o proveedores de dichos servicios, el cual debe incluir:

- Descripción, alcance y duración del servicio.
- Horarios de prestación del servicio.
- Tiempos de respuesta esperados.
- Exclusiones del servicio.
- Acuerdos de Confidencialidad.
- Procedimiento para notificar a la organización incidentes de seguridad de la información.
- Requisitos para manejar los riesgos de seguridad de la información asociados con la cadena de suministro del bien o servicio de tecnología de información o comunicación.
- Auditorias de servicio.
- Requisitos para realizar cambios en la infraestructura tecnológica, procedimientos y controles de seguridad existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos involucrados y la reevaluación de los riesgos.
- Capacidad suficiente.

Estos SLA deben hacer parte integral de los contratos a los que se les aplique estos requerimientos y que se firmen con los proveedores a quienes se les ha tercerizado un servicio.

Antes de realizar cualquier tipo de conexión con terceros, se debe realizar un análisis de los riesgos inherentes a la conexión, condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios, identificando los controles para minimizar el impacto de estos.

Los contratistas, y/o proveedores aceptan y firman el acuerdo de confidencialidad establecido por la organización.

En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.

En el momento de la conexión a los sistemas de información del grupo empresarial y cuando se considere pertinente se debe monitorear el cumplimiento de los SLA, acuerdos de confidencialidad, acuerdos de Intercambio de información y los requisitos de seguridad de la información de parte de los terceros proveedores de servicios.

El oficial de seguridad de la información realiza seguimiento a los proveedores críticos definidos por el BIA, mínimo una vez al año para validar el cumplimiento de las cláusulas y SLA basado en los controles de la norma ISO 27001.

ANEXO No. 9 – POLÍTICA INTERNA DE SEGURIDAD DEL RECURSO HUMANO

ALCANCE/ APLICABILIDAD

La información contenida en el presente documento es de aplicación exclusiva para la Bolsa o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

Responsabilidades

La siguiente política aplica a los colaboradores o terceros del grupo empresarial.

DIRECTRIZ GENERAL

El proceso de Gestión del Talento Humano cumple con todas las políticas y procedimientos de seguridad del recurso humano para avalar que los colaboradores y temporales:

- Conozcan y entiendan sus responsabilidades en cuanto a la seguridad de la información y las funciones del cargo.
- Reduzcan el riesgo de robo, fraude, daño, fuga de información o uso inadecuado de las instalaciones y los servicios de información.

1. VIOLACIONES A LA POLÍTICA Y/O DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

Las violaciones de las políticas y directrices de la Seguridad de la información pueden resultar en acciones de tipo disciplinario que están sujetas a:

- Acción de tipo disciplinario según la directriz establecidas por el Código Sustantivo del Trabajo, el Reglamento Interno de Trabajo, las cláusulas especiales que se establezcan con los colaboradores en sus Contratos Laborales y/o todo aquello que según las leyes colombianas definan como acciones disciplinarias.
- Suspensión o acceso restringido a las áreas de procesamiento de la información, por algún daño causado.
- Terminación del contrato de trabajo o relación comercial (Basados en las disposiciones emitidas por las leyes colombianas en materia laboral).
- Demanda civil o penal.

2. PREVIO A LA CONTRATACIÓN LABORAL

La dirección de Talento y cultura establece el contrato laboral, las funciones y responsabilidades de los colaboradores alineadas con la política y directrices de seguridad del Sistema de Gestión de Seguridad de la Información.

Las responsabilidades incluyen:

- Desarrollar sus funciones de acuerdo con las Políticas y Directrices de Seguridad de la Información establecidas por el grupo empresarial.
- Proteger los activos de información contra el acceso, divulgación, modificación, destrucción o interferencia no autorizada.
- cumplimiento a los procedimientos, instructivos o actividades de seguridad de la información inherentes a su cargo.
- Notificar la pérdida o divulgación de información sensible o cualquier riesgo relacionado con el incumplimiento de los objetivos organizacionales.

Adicionalmente esta área:

Valida los requisitos definidos en el perfil y descripción de cargo en cuanto a educación, formación y/o experiencia y aplica pruebas específicas necesarias para la contratación del colaborador.
Realiza las validaciones con respecto a los antecedentes judiciales sobre los candidatos que permitan generar señales de alerta temprana y tomar decisiones de manera preventiva sobre la continuidad de un proceso.

Protege la confidencialidad y privacidad de los datos de los colaboradores y terceros que estén bajo su responsabilidad.

Establece el programa anual de desarrollo humano y capacitación el cual se ejecuta con la aprobación presupuestal.

La Vicepresidencia de riesgos y cumplimiento en coordinación con la dirección de talento humano y cultura desarrollará el programa de capacitación y concienciación en Seguridad de la Información y ciberseguridad acorde a la disponibilidad del programa anual definido para el grupo empresarial.

Es responsabilidad de los colaboradores el uso apropiado de los activos de información del grupo empresarial que le sean compartidos, conforme a las políticas / directrices de seguridad de la información del grupo empresarial.

Es responsabilidad de los terceros que apoyen el proceso de Talento Humano el cumplimiento de las políticas / directrices de Seguridad de la Información y los aspectos de servicio contemplados en los contratos suscritos.

3. SELECCIÓN

El proceso de Gestión Humana se encarga de que los colaboradores a contratar y/o contratados cumplan con el proceso de selección del personal adecuado rigiéndose por los requisitos de formación, educación y/o experiencia definidos en el formato de perfil y descripción de cargo.

1. Términos y condiciones laborales

Acuerdos de confidencialidad: Los colaboradores firman un acuerdo de confidencialidad y no divulgación de la información.

El acuerdo se firma antes de la divulgación de la información o antes de comenzar las actividades; si ya han comenzado las actividades, la firma del acuerdo debe ser una condición para continuar.

Todo colaborador o tercero se compromete a cumplir con las disposiciones legales e internas respecto a la seguridad de la información, incluyendo responsabilidades para el manejo de información recibida de otras partes, clasificación y protección de esta.

La Vicepresidencia de talento humano y gestión administrativa comunica a los colaboradores, o tercero cuales son las acciones a tomar si hacen caso omiso de los requerimientos de seguridad de la información del grupo empresarial.

El grupo empresarial toma las medidas necesarias para proteger la información personal recolectada a través del proceso de selección y durante la vigencia de la contratación del personal.

4. Durante la vigencia del Contrato

En el proceso de inducción para cada nuevo colaborador del grupo empresarial, cada responsable del proceso debe:

- Informar sobre las funciones y responsabilidades de cada uno de los cargos, incluyendo las responsabilidades en cuanto a la seguridad de la información.
- Concientizar a los nuevos colaboradores sobre la importancia de la seguridad de la información en el desarrollo de sus funciones.
- Directrices del grupo empresarial.
- Entrenamiento en el cargo.
- Divulgación de procedimientos, políticas, directrices y demás documentación de Seguridad de la Información
- Informar sobre las acciones que se efectúan en el grupo empresarial para sancionar los incumplimientos de seguridad de la información por parte de los colaboradores.

5. Terminación o cambio de la contratación laboral

El proceso de gestión humana establece los procedimientos y requerimientos para la terminación o cambio del contrato laboral.

Es responsabilidad de los líderes de proceso verificar y asegurar que todos los colaboradores o terceros devuelvan todos los activos de información que se asignaron y sean propiedad del grupo empresarial, cuando se termine su contratación laboral, contrato de prestación de servicios o acuerdo.

Los derechos de acceso otorgados a los colaboradores, contratistas o terceras partes se retiran tan pronto se termine su relación contractual, o los mismos se modifican después de cualquier cambio en el cargo (cambio de rol o de área) u objeto de contratación.

ANEXO No. 10 – POLÍTICA INTERNA DE SEGURIDAD FÍSICA Y DEL ENTORNO

ALCANCE/ APLICABILIDAD

La siguiente directriz se aplica a todos los colaboradores y/o terceros que tengan acceso a las áreas restringidas del grupo empresarial.

La información contenida en el presente documento es de aplicación exclusiva para la Bolsa o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

RESPONSABILIDADES

Esta política es de estricto cumplimiento para todos los empleados, contratistas y terceros que interactúen con las instalaciones físicas del Grupo empresarial.

DIRECTRIZ GENERAL

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del grupo empresarial. Así mismo, evita el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

El grupo empresarial utiliza perímetros de seguridad para proteger las áreas que contienen instalaciones que soportan el procesamiento de información, cuartos de comunicaciones, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

La Vicepresidencia de Tecnología y los propietarios de la información, cumplen con las disposiciones de seguridad física y ambiental indicadas en la presente directriz. Los gerentes o directores de las áreas definen los niveles de acceso físico de los colaboradores del grupo empresarial a las áreas restringidas bajo su responsabilidad. La Vicepresidencia de talento humano y gestión administrativa será la responsable de la seguridad física del grupo empresarial y atiende los requerimientos de todas las áreas de acuerdo con lo definido en este párrafo.

Las áreas protegidas están restringidas mediante el empleo de mecanismos de control de acceso, mecanismos administrados por la Vicepresidencia Financiera, junto con el director respectivo, permitiendo el acceso sólo a colaboradores autorizados, garantizando la trazabilidad de ingreso y egreso, así como el registro (log) seguro que permita realizar auditorías.

Toda área considerada por el grupo empresarial de acceso restringido cumple con las políticas y procedimientos de seguridad física y del entorno, protegiendo los activos de información frente a pérdida o daño y evitar el acceso no autorizado.

Un área de acceso restringido es aquella en la cual se tienen activos de información clasificados de criticidad alta de acuerdo con el inventario de activos de información.

1. ÁREAS SEGURAS Y PERÍMETROS DE SEGURIDAD FÍSICA

Toda área, oficina o centro de cómputo donde se procese o almacene información del grupo empresarial está dentro de un perímetro de seguridad con las barreras físicas (puertas, torniquetes, biométricos, muros, etc.) suficientes y adecuadas. Dependiendo del nivel de riesgo de los activos de información allí localizados se podrán establecer o no controles que restrinjan el acceso a personas no autorizadas.

La Vicepresidencia Financiera y Administrativa es la responsable de la seguridad física de la información. El acceso a las instalaciones del grupo empresarial es contralado de acuerdo con los procedimientos y mecanismos establecidos por esta vicepresidencia, los cuales se basarán en un análisis de riesgos.

Siempre se identifican y categorizan los requerimientos de seguridad de toda área donde se vaya a procesar o almacenar información del grupo empresarial.

El acceso a las áreas restringidas es únicamente permitido al personal autorizado del grupo empresarial o terceros que cuenten con la debida autorización y siempre en compañía de un colaborador del grupo empresarial.

La autorización para acceder a las áreas restringidas debe ser efectuada teniendo en cuenta el Need-to-know (necesidad del saber).

2. CONTROLES DE ACCESO FÍSICO

Las puertas de acceso a las oficinas del grupo empresarial, las áreas restringidas y cuartos de comunicaciones permanecen cerradas en todo momento. En caso de una falla eléctrica se cuenta con mecanismos de contingencia que garanticen la seguridad de las instalaciones.

Los visitantes permanecen siempre acompañados por un colaborador del grupo empresarial. Si se observan visitantes sin acompañante se notifican a la recepción.

El sistema de circuito cerrado de televisión CCTV es gestionado por el proceso Administrativo y tiene la responsabilidad el mantenimiento de los equipos, realización de los backups y los accesos a las grabaciones.

El proceso administrativo es responsable de realizar el monitoreo del CCTV. En caso de solicitud de una grabación para un caso o investigación, se debe tener el visto bueno del responsable del proceso Jurídico.

3. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES

Las áreas restringidas cuentan con un sistema y sensor contra incendios y su ubicación es de fácil acceso en caso de emergencia. Los sistemas contra incendios son probados conforme a las recomendaciones dadas por el fabricante.

No se almacena en las áreas restringidas sustancias combustibles o peligrosas, ni suministros de papelería a granel a excepción de las áreas destinadas para el manejo de correspondencia.

Se controla y mantienen las condiciones ambientales adecuadas de las áreas para asegurar el buen funcionamiento de los sistemas de procesamiento de información.

La Vicepresidencia de Tecnología verifica que los proveedores que brindan el servicio de almacenamiento y procesamiento de información cuenten con adecuados controles ambientales.

4. ACCESO PÚBLICO

El grupo empresarial controla el acceso público a sus oficinas y áreas restringidas a través de los mecanismos de control previamente definidos.

Todo equipo o dispositivo (Se refiere a computadores personales tipo laptop o desktop y las denominadas tabletas) de terceros que ingrese o se retire de las oficinas del grupo empresarial se deja registro de ingreso del equipo en el formato definido para este fin.

5. SEGURIDAD DE LOS EQUIPOS

Ubicación y protección de los equipos

Los equipos del grupo empresarial son protegidos contra amenazas de tipo físico y ambiental y se ubican en lugares donde se evite el acceso no autorizado.

Existe acceso controlado a los cuartos donde se ubiquen computadores y servidores con información sensible del grupo empresarial.

En todas las áreas donde haya equipos (servidores y equipos de telecomunicaciones) del grupo empresarial, se monitorean los sistemas de regulación de temperatura y humedad de acuerdo con las recomendaciones de los fabricantes, para evitar el sobrecalentamiento de los equipos y fallos en el sistema.

Servicios de suministro

El suministro alterno de energía es adecuado para soportar como mínimo las actividades informáticas definidas como críticas en el BIA (Business Impact Analysis), cuando exista una interrupción en el suministro principal de energía.

El grupo empresarial cuenta con la capacidad suficiente en UPS, para prestar el servicio de fluido eléctrico a los procesos y equipos críticos, en caso de que la fuente de suministro principal falle.

La Vicepresidencia de tecnología realiza revisiones periódicas de las UPS para garantizar que estén en óptimas condiciones, tenga un buen funcionamiento y la capacidad suficiente para soportar el sistema.

Se considera un generador de emergencia si se requiere que el procesamiento continué en el caso de una falla de energía y se dispone de un adecuado suministro de combustible para asegurar que el generador pueda funcionar durante un período prolongado.

Seguridad del cableado

Las conexiones de potencia cuentan con un polo a tierra.
Se cuenta con marcadores de cables (datos y eléctricos) y equipos claramente identificables para minimizar errores en el manejo de estos.

Se cuenta con documentación actualizada de las conexiones de red.

Retiro e ingreso de activos

Al retirarse un equipo del grupo empresarial se protege la confidencialidad, integridad y disponibilidad de la información que contenga.

Los equipos de cómputo, equipos portátiles y cualquier activo de tecnología de la información podrán salir y entrar a las instalaciones del grupo empresarial mediante el registro del equipo en la bitácora ubicada en la recepción del grupo empresarial, siendo la Vicepresidencia Financiera y Administrativa la responsable de resguardar esta bitácora.

El colaborador vela por la seguridad de todo dispositivo que contenga información del grupo empresarial cuando este sea retirado de las instalaciones y toma medidas preventivas para el buen uso de este.

Disposición segura o reutilización de equipos

Antes de reasignar un equipo a otro colaborador, la Vicepresidencia de tecnología genera una copia de seguridad de la información confidencial almacenada en los medios, incluyendo el correo electrónico y se envía / asigna al dueño del proceso al que corresponda dicha información cuando sea requerido.

Cuando se reutilicen equipos o medios de almacenamiento de información se garantiza que se hayan eliminado datos sensibles (formateo) o que se hayan sobrescrito de forma segura.

Si se dan de baja los equipos o medios de almacenamiento de información que se sobrescriben de manera segura, de acuerdo con los procedimientos que defina la Vicepresidencia de tecnología.

Los medios y equipos donde se almacena procesan o comunica la información, se mantiene con las medidas de protección físicas y lógicas que permitan su monitoreo y correcto estado de funcionamiento, para ello se realiza los mantenimientos preventivos y correctivos que se requieran.

Equipos de usuarios desatendidos

Si el usuario abandona la estación de trabajo momentáneamente activa el protector de pantalla con contraseñas, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

Si los sistemas de información detectan inactividad por un periodo de 5 minutos, automáticamente aplica el bloqueo de sesión de usuario.

ANEXO No. 11 – POLÍTICA INTERNA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGUIRDAD

ALCANCE

Esta política aplica para todos los usuarios y/o clientes que procesan información en los activos de información del grupo empresarial y logran identificar eventos que pueden comprometer la seguridad de la información.
La información contenida en el presente documento es de aplicación exclusiva para la Bolsa o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

RESPONSABILIDADES

Todos los colaboradores de la organización que interactúan o tienen conciencia de un evento y/o incidente de Ciberseguridad que involucren activos de información.

GENERALIDADES

1. **NORMAS GENERALES**

Se realiza un proceso de concientización con funcionarios, contratistas, clientes y proveedores, acerca de los tipos de eventos e incidentes relacionados en este procedimiento y los canales correspondientes para el reporte de estos.

2. **ROLES Y RESPONSABILIDADES**

Conforme a lo definido en la política general de seguridad de la información y ciberseguridad, las directrices en esta materia, así como, en la matriz RACI, estos son los roles y responsabilidades establecidos frente a la gestión de los incidentes de ciberseguridad, para la Vicepresidencia de Riesgos y cumplimiento, dirección de aseguramiento y el profesional de seguridad de la información.

Requerimiento	Fase	Actividades	ROL responsable de la actividad
Gestión de incidentes de seguridad y ciberseguridad	Planear	Definir la estrategia (lineamientos / procedimientos) de gestión de incidentes de seguridad de la información y la ciberseguridad	Dirección de riesgos
		Establecer procedimientos (playbooks) de respuesta a incidentes cibernéticos y de seguridad informática e información	Dirección de riesgos
	Hacer	Reportar Incidentes de la ciberseguridad y seguridad de la información	Partes interesadas
		Reportar a la Junta Directiva el resumen de los incidentes de ciberseguridad que afectaron la Entidad	Comité de riesgos
		Realizar la gestión de incidentes de seguridad de la información y la ciberseguridad / seguridad informática	Profesional de seguridad de la información en conjunto con el líder del proceso afectado
		Aplicar las opciones de tratamiento acordadas	Líderes de los procesos a cargo de la opción de tratamiento
	Verificar	Verificar el cumplimiento del procedimiento de gestión de incidentes y que se aplicaron las opciones de tratamiento	Profesional de seguridad de la información en conjunto con el líder del proceso afectado
	Actuar	Implementar mejoras y/o ajustes sobre la estrategia de gestión de incidentes	Vicepresidente de riesgos y cumplimiento

4. CATEGORÍAS Y SUBCATEGORÍAS DE INCIDENTES DE CIBERSEGURIDAD

El grupo empresarial ha establecido las siguientes categorías y subcategorías de incidentes para la categorización y atención de los incidentes:

CATEGORÍA DE INCIDENTE	SUBCATEGORIA DE INCIDENTE	DESCRIPCIÓN
ATAQUES CIBERNÉTICOS DIRIGIDOS	• Whaling • Ingeniera Social • Spear Phishing • APT: Amenaza Persistente Avanzada • AVT: Amenaza volátil avanzada • Espionaje industrial • Robo de propiedad intelectual	Se considera un ataque dirigido a aquel donde los individuos o la organización objetivo están intencionadamente elegidos. La amenaza dirige sus esfuerzos, buscando mantenerse anónima mientras logra el objetivo deseado.
CODIGO MALICIOSO (MALWARE)	• Infección Extendida	Ransomware, Crypto Miner, BOTS, Rootkit, worm o troyano que infecta exitosamente a un conjunto amplio de usuarios, equipos o sistemas.

CATEGORÍA DE INCIDENTE	SUBCATEGORIA DE INCIDENTE	DESCRIPCIÓN
	• Infección Única	Un código malicioso que afecta a un dispositivo y/o usuario del sistema.
DISRUPCIÓN DE SISTEMAS	• Denegación de servicio (DOS/DDOS)	Busca afectar la disponibilidad de un servicio, proceso o sistema de información, a través de la explotación de vulnerabilidades o por medio del envío masivo de grandes cantidades de tráfico y/o peticiones, generando como resultado la imposibilidad del sistema de responder las peticiones de servicio de los usuarios legítimos.
	• Indisponibilidad de servicios de proveedores críticos	Interrupción en los servicios prestados por los proveedores críticos, debido a un ataque: Cloud/hosting/canales de comunicaciones/internet.
ACCESO NO AUTORIZADO	• Inyección SQL • Intentos de login • Cuentas de usuario comprometidas • Elevación de privilegios	Se origina cuando una persona interna o externa obtiene acceso lógico o físico no autorizado a un equipo, aplicación, sistema de información, dato o cualquier recurso técnico
PRUEBAS Y RECONOCIMIENTO	• Scanning • Sniffing	Acciones de reconocimiento que permiten la identificación de recursos corporativos, puertos abiertos, aplicaciones, servicios, cuentas de usuarios, datos, o una combinación de estos.
USO NO AUTORIZADO DEL SISTEMA	• Cryptojacking • Botnet	Emplear los recursos tecnológicos para efectuar ataques o generar transacciones asociadas con criptomonedas.
USO INDEBIDO DE LA MARCA	• Suplantación de sitio web • Registro de DNS • Suplantación de cuentas. • Phishing	Uso de elementos identificativos de elementos de la marca corporativa (logos, imágenes, página web etc.) en cualquier intento fraudulento para adquirir información sensible, como usuarios, contraseñas o cualquier otra información personal que permitan al atacante hacerse pasar por la organización legítima víctima del incidente.
MODIFICACIÓN Y/O ALTERACIÓN NO AUTORIZADA	• Modificación no autorizada de la infraestructura. • Agregar, alterar, o eliminar información clave.	Hace referencia a las siguientes acciones: Alterar, Falsificar, Introducir, eliminar, información o los medios de procesamiento.
CIBERSABOTAJE	• Hacktivismo • Noticias Falsas • Campañas negativas • Exempleados	Hace referencia ataques de impacto reputacional en redes sociales o portales a través de noticias falsas o campañas negativas.
EXPLOTACIÓN DE VULNERABILIDADES	• Nativa	Incidente provocado por la explotación de una vulnerabilidad desconocida por el fabricante, por ejemplo: Vulnerabilidades relacionadas al día 0.
	• Mala configuración	Configuración inadecuada de los sistemas de información, por medio de las cuales se puedan

CATEGORÍA DE INCIDENTE	SUBCATEGORIA DE INCIDENTE	DESCRIPCIÓN
		realizar acciones no autorizadas. Por Ejemplo: Contraseñas por defecto, protocolos vulnerables, etc.
	• Sistema No Actualizado	Cualquier tipo de incidente provocado por la explotación de una vulnerabilidad conocida, publicada y solucionada por el fabricante de la plataforma, pero que no se encuentra aplicada sobre la plataforma o sistema.

5. CATEGORÍAS DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Las siguientes son las categorías de los incidentes definidas por el grupo empresarial:

- Incumplimiento de las Políticas de Seguridad.
- Quebrantamiento de las disposiciones de Seguridad Física.
- Pérdida o fuga de información.
- Pérdida o alteración física de equipos.
- Uso inadecuado de los sistemas de información.
- Cambios no controlados en los sistemas de información.
- Mal funcionamiento del software o del hardware.

6. CRITERIO DE CLASIFICACION DE UN INCIDENTE

Para clasificar un evento como incidente se debe tener en cuenta las 3 premisas de Seguridad de la Información:

Confidencialidad

Si el evento viola las políticas de Seguridad de la información o vulnera los controles de seguridad de la información, permitiendo, la filtración de información de las bases de datos productivas y/o revelación información estratégica, técnica, datos privados acorde con ley 1581 de 2012 o información clasificada como crítica para la organización usando cualquier categoría indicada en el numeral 4.3 o 4.4.

Integridad

Si el evento viola las políticas de Seguridad de la información o vulnera los controles de seguridad de la información, permitiendo, realizar una modificación no controlada en producción que impide o altere los procesos productivos de la organización y su corrección requiera un análisis técnico de la data productiva o compromiso de los archivos de auditoría del activo de información, usando cualquier categoría indicada en el numeral 4.3 o 4.4.

Disponibilidad

Si el evento viola las políticas de Seguridad de la Información o vulnera los controles de seguridad de la información, generando una interrupción abrupta no controlada que supere los umbrales y casuística definida en el plan de continuidad del negocio la cual impida realizar sus procesos misionales y esta interrupción afecte directamente a los clientes en los acuerdos contractuales firmados, usando cualquier categoría indicada en el numeral 4.3 o 4.4.

7. TABLA DE DEFINICION DE CRITICIDAD DE UN INCIDENTE

Clasificación	Confidencialidad	Integridad	Disponibilidad
Nulo	Los controles son adecuados y no hay perdida de Información crítica.	No hay compromiso de modificación de base de datos productivas	No hay interrupción de la operación misional de la
Bajo	La información comprometida es fácilmente recuperable y no compromete la estrategia de la organización o datos semiprivados de los clientes.	La información comprometida tiene backup habilitado con un periodo menor a 24 horas del incidente, la recuperación o construcción de la información se puede realizar sin reprocesos.	Se tiene una interrupción controlada y tiene un sistema de marcha atrás definido.
Medio	La información comprometida requiere de esfuerzo operativo para su recuperación, no compromete la estrategia de la organización o puede comprometer datos semiprivados de los clientes.	La información comprometida tiene backup habilitado con un periodo menor a 48 horas del incidente, la recuperación o construcción de la información requiere realizar reprocesos operativos.	Se tiene una interrupción controlada y tiene un sistema de marcha atrás definido, pero puede tardar y afectar a los clientes.
Alto	La información comprometida es parcialmente o irrecuperable, compromete la estrategia de la organización, compromete datos privados de los clientes.	La información comprometida no tiene backup o se puede recuperar parcialmente con un periodo mayor a 1 Semana del incidente, la recuperación o construcción de la información requiere realizar reprocesos.	Se tiene una interrupción no controlada y no se tiene marcha atrás definido, controlado afecta a los clientes.

8. CRITERIO DE EVALUACIÓN DE UN INCIDENTE

Confidencialidad	Integridad	Disponibilidad
0	0	0
1	1	1
2	2	2
3	3	3

Nivel de criticidad establecido:

Criticidad	Puntaje	Descripción
Alto	9-7	La organización ya no puede proporcionar uno o más servicios críticos a ningún usuario,

Criticidad	Puntaje	Descripción
		o se ha comprometido la seguridad de datos personales privados.
Medio	6-4	La organización ha perdido la capacidad de proporcionar un servicio crítico a un subconjunto de usuarios del sistema
Bajo	3-1	Efecto mínimo; la organización todavía puede proporcionar todos los servicios críticos a todos los usuarios, pero ha perdido eficiencia.
Nulo	0	No se afecta la capacidad de la Compañía para proporcionar todos los servicios críticos a todos los usuarios.

9. REPORTE SOBRE EVENTOS, INCIDENTES Y VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Todas las personas que tengan acceso a la información del grupo empresarial tienen la obligación de comunicar oportunamente, apenas se tenga conocimiento de la situación, cualquier evento o incidente de seguridad de la información o ciberseguridad según lo definido en el presente documento a la Vicepresidencia de Riesgos de acuerdo con el procedimiento que se señala más adelante en este documento.

Adicionalmente, todas las vulnerabilidades del sistema de seguridad de la información o ciberseguridad deben ser informadas a la Vicepresidencia de Riesgos y cumplimiento a la cuenta de correo riesgooperativosfc@bolsamercantil.com.co.

10. GESTIÓN DE LOS INCIDENTES Y LAS MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Cada vez que sea comunicado a la Vicepresidencia de Riesgos y cumplimiento un incidente de seguridad, evento de seguridad, ciberataque, debilidad o sospecha de su ocurrencia, debe seguirse el procedimiento que se describe más adelante.

Para este fin, el grupo empresarial ha establecido un Sistema de Comando de Incidentes (SCI) transversal, que tiene por objetivo brindar solución temporal o definitiva a cualquier incidente presentado de impacto **ALTO** que produzca una interrupción en la continuidad del negocio y la prestación del servicio de los procesos vitales, emergencias con afectación a los colaboradores y/o daños a la infraestructura del grupo empresarial , afectación de la reputación, seguridad de la información y ciberseguridad que permita minimizar los impactos negativos en la organización- El SCI será convocado cuando la gravedad del incidente así lo requiera.

El Sistema de Comando de Incidentes siempre adelanta una gestión transparente, verídica, confiable e imparcial, cumpliendo con la legislación vigente y garantizando la integridad de sus acciones de acuerdo con las disposiciones especificadas en los lineamientos internos de Seguridad de la Información del grupo empresarial y la legislación que aplique.

11. ETAPAS COMUNES EN LOS CIBERATAQUES

Es necesario dentro de la gestión de incidentes de ciberseguridad y de la información y en particular en la fase de preparación, conocer las fases que componen los ataques cibernéticos. El siguiente gráfico detalla las tres fases comunes de un ataque cibernético: Reconocimiento, propósito y ataque.

12. APRENDIZAJE DEBIDO A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El Oficial de Seguridad de la Información:

- Mantiene indicadores de los incidentes de seguridad y el impacto que los mismos ocasionan en el grupo empresarial.
- Gestiona la actualización de la matriz de riesgos de seguridad de la información y/o ciberseguridad junto con sus controles, teniendo como referencia los indicadores sobre incidentes de seguridad.

13. RECOLECCIÓN DE EVIDENCIAS

Si la evidencia se encuentra en medio digital, el Oficial de Seguridad de la Información realiza copias de respaldo y garantizar la no modificación de la data.
Si se detecta un evento o incidente de seguridad que puede generar una acción o proceso legal, se deben tener en cuenta los siguientes requisitos en cuanto a las evidencias:

- Admisibilidad de la evidencia: Si la evidencia se puede o no utilizar en el proceso para lo cual se solicita apoyo del abogado del grupo empresarial, los contactos de autoridades definidos y el apoyo de un consultor externo en caso de que se considere necesario.

- Peso de la evidencia: Calidad e integridad de la evidencia. El Sistema de Comando de Incidentes garantiza:

  - Procesamiento y almacenamiento seguro de la evidencia.
  - Copias de seguridad de la evidencia original.
  - Control de acceso a las evidencias recolectadas.
  - La evidencia no ha sido alterada.
  - Documentos en papel: se almacena con las respectivas medias de seguridad y se registra quién encontró el documento, cuándo y dónde lo encontró.
  - Medios de computador: se realiza duplicados o copias de la evidencia para garantizar la disponibilidad de la información, la evidencia se cifra para garantizar la confidencialidad y se registra todas las actividades realizadas durante el proceso de copiado. Si no es posible realizar un duplicado se conserva intactos y de manera de segura.
  - Cuando se realice investigación forense, la misma se realiza en duplicados de la evidencia; para evitar el daño o modificación del original. Ante un análisis forense, los sistemas y/o equipos afectados se dejan quietos, para evitar pérdidas de evidencia, por su manipulación.

14. TIEMPOS DE RESPUESTA

Para el caso de la atención de incidentes de seguridad de la información se han establecido unos tiempos máximos de atención de estos, con el fin de atender adecuadamente los incidentes de acuerdo con su criticidad e impacto.

Los tiempos expresados en la siguiente tabla son un acercamiento al tiempo máximo en que el incidente se atenderá una vez se conozca del mismo, y no al tiempo en el cual el incidente se soluciona; esto se da a que la solución de los incidentes puede variar dependiendo del caso.

Nivel de impacto	Tiempo máximo de atención
Alto	Inmediata, Máximo 30 minutos
Medio	Entre ocho horas y 2 días
Bajo	Entre 2 y 3 días

Acciones Posteriores:

Las acciones posteriores a la contención del incidente están a cargo del profesional de seguridad de la información e incluyen documentar el incidente de seguridad que se encontrará dentro de la herramienta de gestión de incidentes (BPM / CERO) y dependiendo del grado del incidente (Alto o Medio), se reporta al Comité de Riesgos en cuya sustentación podrá ser requerida la presencia del área que aplicó la solución.

El formato incluye:

- Detalles de la persona que hace el reporte
- Descripción del incidente de seguridad de la información
    - Qué ocurrió
    - Cómo ocurrió
    - Por qué ocurrió
    - Componentes Afectados
    - Impactos adversos al negocio
    - Vulnerabilidades explotadas
- Detalles del incidente de seguridad de la información
    - Fecha y Hora de ocurrencia del incidente
    - Fecha y Hora de descubrimiento del incidente
    - Fecha y Hora de reporte del incidente
    - ¿El evento se encuentra en curso?
    - Tiempo de duración del incidente
- Detalles de los miembros del equipo que trabajaron en el informe
- Bienes afectados
    - Bienes y recursos identificados como afectados dentro de la gestión del incidente
- Impacto / Efecto del incidente adverso para el negocio
    - Incumplimiento de la confidencialidad (es decir divulgación no autorizada)
    - Incumplimiento en la integridad (es decir, modificación no autorizada)
    - Incumplimiento en la disponibilidad (es decir, no disponibilidad)
    - Incumplimiento de No-Repudio
    - Destrucción
- Solución del incidente
    - Documentación general del incidente
    - Acciones emprendidas para solucionar el incidente

- Ninguna acción
- Acción Interna
- Acción Externa
- Investigación Interna
- Investigación Externa

- Acciones Planificadas para solucionar el incidente

  - Ninguna acción
  - Acción Interna
  - Acción Externa
  - Investigación Interna
  - Investigación Externa

- Acciones pendientes

  - Descripción de acciones pendientes con el fin de cerrar por completo el caso de gestión del incidente

1. FASE 3 SEGUIMIENTO

Reportar el incidente a las partes interesadas relevantes; realizar el monitoreo al incidente y la implementación de controles.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1. MONITOREAR LOS INCIDENTES SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD	El Profesional de Seguridad de la Información realiza seguimiento a los incidentes de seguridad de la información y/o Ciberseguridad presentados: • Controla que se implementen las medidas para evitar que el incidente se vuelva a presentar. • Determina si otros sistemas / Información de la compañía son vulnerables al mismo método de ataque. • Formula recomendaciones sobre actualizaciones o cambios en la seguridad. • Evaluar el manejo del incidente para identificar la efectividad de las medidas tomadas.	Profesional Seguridad de la Información.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
2. COMUNICACIONES EXTERNAS SOBRE LOS INCIDENTES DE CIBERSEGURIDAD	Comunica a las partes interesadas que así lo requieran, la gestión de los incidentes, así como las medidas adoptadas para remediar el incidente de acuerdo con lo definido en el Procedimiento de Gestión de Comunicaciones.	Sistema Comando de Incidentes

2. FASE 4 CIERRE Y APRENDIZAJE

Esta fase cubre la identificación de las lecciones aprendidas y la actualización de la información clave, controles y procesos.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
1. CERRAR INCIDENTE	Valida la efectividad de las acciones correctivas y preventivas ejecutadas para la mitigación o erradicación del incidente de Seguridad de la Información y/o Ciberseguridad. Documenta las causas, las actividades ejecutadas, las evidencias recopiladas, las conclusiones y toda la información adicional del panorama del incidente. La gestión y anexos del incidente quedan registrados en la aplicación CERO. Finalizada la gestión del incidente se cambia el estado ha CERRADO. Hacer los ajustes a los procedimientos de manejo de incidentes de acuerdo con las lecciones aprendidas	Profesional Seguridad de la Información.
2. REPORTAR LA GESTIÓN DE INCIDENTES	Semestralmente el Gerente Corporativo de Riesgos con el apoyo del Profesional Seguridad de la Información reportará los resultados de la gestión de los incidentes de seguridad de la información y/o ciberseguridad y el resumen de los incidentes que afectaron a la compañía, al Comité de Riesgos del grupo empresarial; quien a su vez lo reportará a la Junta Directiva.	Gerente Corporativo de Riesgos Profesional Seguridad de la Información.
3. LECCIONES APRENDIDAS	Una vez recuperada la operatividad del sistema, se articulan recomendaciones y oportunidades de mejora que optimicen el nivel de aseguramiento de este para que el administrador del sistema los lleve a cabo a través de un plan. De igual forma se establece comunicación de lecciones que permitan un mejoramiento en el proceso de tratamiento a	Profesional Seguridad de la Información.

ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
	incidentes en seguridad de la información y ciberseguridad con el fin de identificar mejoras en la seguridad de la Compañía: • Identifica tendencias/patrones. • Identifica las áreas de preocupación. • Analiza dónde se podrían tomar acciones preventivas para reducir la probabilidad de incidentes futuro. • Identifica las mejoras en la implementación de controles, como resultado de las lecciones aprendidas. • Realiza pruebas del procedimiento de gestión de incidentes. Socializa, cuando se considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades del sector.	
4. INDICADORES	Se realiza el registro de la solución del caso según las conclusiones del informe de gestión y posterior cierre. Trimestralmente se consolida la información de cuantos incidentes y de qué tipo se presentaron en el grupo empresarial, con el fin de generar el correspondiente indicador para el informe de gestión a la Vicepresidencia de Riesgos y cumplimiento	Profesional Seguridad de la Información.

14. ESTRATEGIA DE COMUNICACIONES (REPORTES)

1. COMUNICACIONES EXTERNAS

El grupo empresarial establece a través del siguiente esquema, la estrategia para las comunicaciones externas; a través del cual se define el contenido a comunicar, a quién o a quienes se comunican, quién lo comunica y cuándo se van a llevar a cabo las comunicaciones.

QUÉ COMUNICAR	A QUIÉNES					CUANDO				VOCERO				
	Entes reguladores	Autoridades	Clientes	Entidades del sector	Proveedores	Por demanda	Mensual	Trimestral	Semestral	Comité de Riesgos	Vicepresidencia de Riesgos y cumplimiento	Sistema Comando Incidentes/Comité De Crisis	Profesional de Seguridad de la información	Dirección de comunicaciones y sostenibilidad
Reporte externo a las autoridades pertenecientes al modelo nacional de gestión de incidentes cibernéticos; de aquellos incidentes cibernéticos mayores o aquellos que la Compañía no consiga contener o erradicar.		X				X					X			
Reporte a la Super Intendencia Financiera de Colombia, sobre los incidentes de ciberseguridad, de acuerdo con lo establecido en el presente documento y en consonancia con las normas por esta expedidas[1].	X					X					X			
Reporte a la Superintendencia de Industria y Comercio a través del RNBD cuando el incidente haya afectado la seguridad de los datos personales[2]	X					X					X			
Reporte de las lecciones aprendidas de los incidentes.				X	X	X							X	
Política de Ciberseguridad.					X	X					X			

QUÉ COMUNICAR	A QUIÉNES					CUANDO				VOCERO				
	Entes reguladores	Autoridades	Clientes	Entidades del sector	Proveedores	Por demanda	Mensual	Trimestral	Semestral	Comité de Riesgos	Vicepresidencia de Riesgos y cumplimiento	Sistema Comando Incidentes/Comité De Crisis	Profesional de Seguridad de la información	Dirección de comunicaciones y sostenibilidad
Reporte externo a los clientes de La , sobre los incidentes cibernéticos que hubiesen afectado la confidencialidad, la integridad o la disponibilidad de su información.			X			X								X

1. CONTACTOS COMUNICACIONES EXTERNAS CON LAS AUTORIDADES

Figura 1

Autoridad	e-mail	Teléfono
Policía Nacional	ponal.csirt@policia.gov.co	5159090
Grupo de Respuestas a Emergencias Cibernéticas de Colombia	contacto@colcert.gov.co	2959897

2. PUNTO DE CONTACTO PARA COMUNICACIONES EXTERNAS CON ENTES REGULADORES

Figura 2

Autoridad	e-mail	Teléfono
Superintendencia Financiera de Colombia	riesgooperativo@superfinanciera.gov.co	5940200

La siguiente taxonomía entrega los lineamientos básicos necesarios para el reporte de incidentes cibernéticos, ofreciendo una estandarización y lenguaje común en el proceso de identificación con las entidades de apoyo como Colcert. Está compuesta de cinco (5) elementos y la clasificación en nueve categorías diferentes que se explican a continuación:

1. Elementos de un Incidente

Es importante la identificación de los elementos involucrados en la materialización de un incidente cibernético, debido a que estos son un factor determinante a la hora de clasificarlo. Si bien es posible que inicialmente no se puedan identificar todos los elementos de manera inmediata, ello se deberá realizar durante la gestión del incidente. Los cinco (5) elementos que deben identificar son:

1. Agentes de Amenaza

Considerado como el elemento causante del incidente. Se le atribuyen las acciones que llevan a la materialización. Ellos son:

- Kiddie
- Hacker – Ciberpunk
- Hacker veterano (Old-timer)
- Guerrero de código (code warrior)
- Ciber ladrón
- Ciber vendedor
- Empleado insatisfecho
- Exempleado
- Ciberacosador
- Estafador
- Crimen organizado
- Combatiente

2. Herramientas

Elementos utilizados por los agentes de amenaza para materializar un incidente. Para su identificación se deben considerar las acciones que se realizaron.

Pueden existir un sin número de herramientas, pero es posible agruparlas en definiciones generales en sus accionares. Ellas son:

- Herramientas físicas
- Scripts
- Agentes autónomos
- Herramienta distribuida
- Desconocida

3. Tácticas y Técnicas

Se definen como el actuar de los agentes de amenaza para llegar a la materialización del incidente. Este elemento define gran parte de la clasificación del incidente dentro de la taxonomía. Se debe identificar y reportar la táctica y la técnica haciendo uso del framework de MITRE denominado ATT&CK y que se encuentra en el siguiente link: https://attack.mitre.org/matrices/enterprise/

4. Activos

A qué elemento fue dirigido el ataque que concluyó con la materialización del incidente. No se tiene una lista definida, pero es posible identificarlo como:

- Servicio
- Proceso
- Información
- Componente de TI
- Estación de Trabajo
- Red

- Otro

5. Propósito Es posible que los agentes de amenaza tengan un fin a cumplir. Este elemento podrá brindar una clara identificación del incidente. Aunque algunas veces no sea fácil determinarlo de manera inmediata, este se puede identificar durante la gestión del incidente. Se tienen como propósitos los siguientes:

- Desafío
- Asuntos políticos
- Pánico
- Ganancia financiera
- Daño
- Espionaje

2. Categorías

Se definen nueve categorías las cuales son utilizadas por la mayoría de los CERT y CSIRT a nivel mundial. Con esto se podrá compartir información con dichas entidades cuando sea necesario.

1. Abuso de contenido

Los incidentes de abuso de contenido son aquellos en que se ve comprometida la imagen de la entidad o corresponden al uso de medios electrónicos de la entidad para realizar acciones que contienen aspectos prohibidos, ilícitos u ofensivos. Dentro de esta categoría pueden encontrarse incidentes como lo es el envío de spam, pornografía infantil, información con contenido explícito o acciones violentas, amenazas, desacreditación o discriminación de alguien (por ejemplo, acecho cibernético, racismo y amenazas contra uno o más individuos).

2. Código Malicioso

Se refiere a un programa o un código de programa destinado a realizar una función o proceso no autorizado que tendrá un impacto adverso en la confidencialidad, integridad o disponibilidad de un sistema de información. Generalmente existe una interacción del usuario necesaria para activar o ejecutar el código.

Se consideran dentro del código malicioso tipos como virus, troyanos, gusanos, spyware, Adware/Hoax, ransomware, rogueware, exploits, entre otros.

3. Recopilación de Información

Técnicas que son usadas por un agente de amenaza y llevadas a cabo como paso previo al ataque a una entidad. Consiste en recabar la máxima cantidad de información de la plataforma tecnológica mediante buscadores, redes sociales, sitios web públicos con contenido filtrado o recopilado, entre otros. Dicha información permite al atacante elaborar un “perfil” de su objetivo, aumentando así las probabilidades de éxito.

Algunos ejemplos serían las acciones como escaneo de puertos, servicios y cuentas (Scanning), observar y grabar tráfico de red (Sniffing), tanto cableada como inalámbrica (ej. Wiretapping), obtención e inspección de información a través de medios no técnicos (ingeniería social), descubrimientos y debilidades basados en fuentes de inteligencia abierta (Técnicas de OSINT), configuraciones por defecto en plataformas de TI, ataques conocidos como Man in the Middle, Sesión Hijacking, entre otros.

4. Intrusiones

Son las acciones tendientes para eludir los mecanismos de autenticación y acceso de un sistema. Contemplan desde un acceso a recursos sin autorización hasta múltiples intentos de inicio de sesión (Adivinar / descifrar contraseñas) o mediante la ejecución de programas o exploits, incluyen ataques conocidos como Poissoning, ataques sobre los sistemas de autenticación y la capacidad de explotación de peticiones (fuerza bruta).

Acciones como intentos o accesos a una cuenta privilegiada, ataques sobre kerberos, ataques Pash the Hash, ataques que busquen adquirir privilegios ilícitos sobre un sistema no autorizado (elevación de privilegios), ataques cuya finalidad es, utilizando un sistema comprometido, atacar los accesibles a través de este (movimiento lateral), ataques que explotan o utilizan técnicas de acceso a través de backdoor en un aplicativo.

Aquellos que se realicen mediante la explotación de vulnerabilidades con un identificador estandarizado como el nombre CVE (por ejemplo, desbordamiento de búfer, puerta trasera, secuencias de comandos entre sitios, etc.) serán catalogados dentro de la categoría de vulnerabilidades.

5. Disponibilidad del Servicio

Se considera cuando la propiedad de la disponibilidad se afecta tanto en el acceso, uso oportuno y confiable de un sistema, aplicación (servicio) o la información misma. Ejemplos de DoS son las inundaciones de ICMP y SYN. DDoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros escenarios como los ataques de Amplificación DNS.

Adicionalmente, la disponibilidad también puede verse afectada por acciones locales (destrucción, interrupción del suministro de energía, etc.), fallas espontáneas o errores humanos, sin malicia o negligencia, y sabotaje, este tipo de situaciones no deberá ser reportado como un incidente de ciberseguridad. Los incidentes que tienen que ser reportados son aquellos mapeados en la matriz MITRE.

6. Fraude

Uso de tecnologías de la información con el fin de distorsionar los datos e inducir a la víctima a hacer alguna actividad o tarea, provocando con ello afectación a la confidencialidad, integridad o disponibilidad de la información. Una forma de fraude involucra la intercepción de una transmisión

electrónica, ocasionando el robo de credenciales, los datos de la tarjeta de crédito u otra información confidencial sobre la identidad de una persona.
Se considera fraude el uso no autorizado de recursos, violación a la propiedad intelectual y derechos de autor (Copyright), enmascaramiento, phishing y spear phishing, spoofing (Suplantación) o alteración y/o eliminación de datos almacenados, entre otros.

7. Seguridad del Contenido de la Información

Se refiere a aquellos incidentes que puedan comprometer la información. Considera acciones como las interceptaciones, acceso o alteración, directa o indirecta, independientemente de su localización, de información no autorizada, fuga o compartición de información sensible o no autorizada, exposición intencionada o no, de información no autorizada, perdida o borrado de información de forma inintencionada, fuga de información sensible a través de los metadatos incrustados en archivos (esteganografía).

8. Vulnerabilidades

Incidentes que son materializados por la explotación de una vulnerabilidad. Se consideran los ataques comunes como lo son XSS (Cross Site Scripting por sus siglas en inglés), SQL Injection, ataques de inyección, Ataques RFI / LFI, ataques CSRF, ataques SSL y certificados, ataques basados en web (Cookie reply, clonación de sesión), vulnerabilidades conocidas, entre otros.
Adicionalmente, se incluyen dentro de esta categoría las acciones que se realizan mediante la explotación de vulnerabilidades con un identificador estandarizado como el nombre CVE (por ejemplo, desbordamiento de búfer, puerta trasera, secuencias de comandos entre sitios, etc.)

9. Otros

Incidentes que no están contemplados en ninguna de las ocho categorías anteriores. Pueden ser un indicador para la actualización de la clasificación.

ANEXO No. 12 – POLÍTICA INTERNA DE MONITOREO DE ALERTAS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

ALCANCE

El monitoreo aplica para las alertas que se reciban de las herramientas de Ciberseguridad o sistemas de información: office 365 módulo de security y compliance, Trend Micro (Apex One / vision One), Firewall oficina, Servicio SOC proveedor externo, tickets y notificaciones de los servicios de Ciberseguridad de AWS, así como otras herramientas que se lleguen a configurar que refuercen la seguridad de la información y ciberseguridad del grupo empresarial

La información contenida en el presente documento es de aplicación exclusiva para la Bolsa o para cada una de las empresas que conforman el grupo empresarial, según corresponda.

RESPONSABILIDADES

La vicepresidencia de Riesgos y cumplimiento a través del equipo de seguridad de la información realizará la supervisión y monitoreo de eventos y posibles incidentes de ciberseguridad que amenacen la integridad, confidencialidad y disponibilidad de la información del grupo empresarial

La vicepresidencia de Tecnología realizará las validaciones y verificaciones de las alertas reportadas y justificará o sustentará cada uno de los eventos reportados por Seguridad de la Información.

GENERALIDADES

GESTIÓN DE ALERTAS DE ACUERDO CON SU CRITICIDAD

1. GESTIÓN DE ALERTAS

Las herramientas de ciberseguridad y servicios asociados a este envían diariamente alertas y notificaciones sobre posibles eventos de ciberataques. Para la adecuada gestión de las alertas se definen los siguientes aspectos:

- Se atienden las alertas con calificación High, Alta, Critical, Urgent o calificación superior a 80 dependiendo de cada sistema.
- Se atienden las alertas de virus o malware que generen propagación a varios usuarios o sistemas de información de la compañía, así no tengan alguna de las calificaciones antes mencionadas.
- Se atienden tickets del servicio de SOC con calificación High, Critical o Urgent.
- Las alertas o tickets con calificación inferior a High, Alta, Critical, Urgent u 80, no serán gestionadas al menos que afecten la confidencialidad, integridad y disponibilidad de un activo que esté calificado como crítico en la matriz de activos de información o afecten un proceso vital considerado así en el Sistema de Gestión de Continuidad del Negocio.

2. ACUERDO DE NIVELES DE SERVICIO PARA LA GESTIÓN DE ALERTAS

Las alertas o tickets con calificación High, Alta, Critical, Urgent u 80, son gestionadas dentro de las 24 horas una vez recibida la alerta.

Los procesos y herramientas deben asegurar el reporte inmediato de las alertas para gestionarlas de manera oportuna.

INSTRUCTIVOS DE MONITOREOS

Para la realización de los monitoreos de las alertas se debe realizar la ejecución de los siguientes instructivos de acuerdos con el tipo de monitoreo.

- Instructivo monitoreo de usuarios con acceso a VPN
- Instructivo monitoreo de software instalado en equipos de cómputo
- Instructivo monitoreo de alertas antivirus/antimalware
- Instructivo monitoreo de alertas directorio activo y actividades de usuarios administradores

- Instructivo de monitoreo de alertas servicio de SOC de Rackspace y gestión de tickets AWS
- Instructivo para obtener información en la realización de monitoreo de usuarios y perfiles y actividades de los usuarios administradores

ANEXO No. 13 – POLÍTICA INTERNA DE ESCRITORIO Y PANTALLA LIMPIA

Objetivo

La organización establece las directrices de escritorio y pantalla limpios con el propósito de reducir los riesgos de perdida, modificación y acceso no controlado de la información, durante y fuera de las actividades laborales.

Alcance

Esta política aplica para todos los activos de información digital y físicos de la organización y sus Filiales de obligatorio cumplimiento de todos los empleados, contratistas y terceros que desempeñen y ejecuten labores y funciones en la compañía.

Responsabilidades

Todos los colaboradores de la bolsa a los cuales se le asignen equipo de cómputo y recurso office 365.

Generalidades de la política

Los dueños de activos de información son responsables de proteger el acceso no controlado a los repositorios donde se encuentran alojada la información sea físico o lógico, el desconocimiento o no uso de estos es sancionado de acuerdo con el procedimiento definido.

Responsabilidades generales

- La responsabilidad del acceso a equipos de cómputo, cualquier sistema o aplicativo de la organización, mientras este activo es del usuario al cual se le asigno por parte del dueño del Activo de Información o la vicepresidencia de Tecnología.
- Cualquier acceso, modificación o exfiltración de información estará bajo la responsabilidad del dueño del acceso.
- Los usuarios deben terminar la sesión y bloquear su equipo de cómputo cuando finalicen su turno o estén ausentes de forma temporal de su puesto de trabajo.
- Informar sobre cualquier incumplimiento o evento anormal en el funcionamiento de su equipo de cómputo a la Vicepresidencia de Riesgos.
- La vicepresidencia de Tecnología activará y mantendrá los controles en caso