POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INDICE

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La organización Clínica Bonnadona Prevenir, en adelante OCBP, determina la información como un activo de alta importancia para la entidad, indispensable para alcanzar los objetivos estratégicos de la organización. Por consiguiente, es necesario disponer de estrategias, lineamientos y reglas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

En la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas.

2. OBJETIVO

El objetivo principal de la presente política es definir los principios, procedimientos, lineamientos, mecanismos y reglas básicas para proteger, conservar y asegurar los recursos de información de la Organización.

2.1 OBJETIVO ESPECIFICO

- Determinar las medidas esenciales de seguridad de la información que la organización debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información.
- Aplicar barreras y procedimientos que resguarden el acceso a los datos solo para las personas autorizadas.
- Gestionar la adquisición de software, control, desarrollo de aplicaciones propias y uso de aplicaciones externas.
- Definir una estrategia de continuidad de los procesos de la entidad frente a incidentes de seguridad de la Información.
- Proteger los activos de información de la organización.
- Trasmitir la información de la Organización de manera segura.
- Evitar alteraciones indebidas en la información.
- Fortalecer la cultura de seguridad de la información en funcionarios, terceros y, clientes mediante la definición de una estrategia de uso y apropiación de la política

3. ALCANCE

Esta política se aplica a todo el personal de Organización Clínica Bonnadona Prevenir y todas sus sedes, independiente del modelo de contratación, y también al personal externo que preste o prestare servicios, remunerados o no, a la organización como consultores, asesores, auditores, terceras partes, etc. También es aplicable a todo activo de información que la organización posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger estos activos de información.

La política cubre toda la información, entre otros, la impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, o hablada en una conversación.

La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización basándose en metodologías de mejoramiento continuo. Este proceso de gestión deberá ser aplicado a todos los procesos de negocio de la organización

Esta política es de estricto cumplimiento y cuenta con mecanismos de control y de sanciones asociadas al no cumplimiento.

4. DEFINICIONES

- **Acceso remoto**: Un acceso remoto es poder acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa.
- **Activo:** Según [ISO IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la OCBP
- **Administración de incidentes de seguridad:** Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.
- **Almacenamiento en la Nube**: es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet.
- **Amenaza**: Según [ISO IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Análisis de riesgos**: A partir del riesgo definido, se define las causas del uso sistemático de la Información para identificar fuentes y estimar el riesgo.
- **Autenticación**: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Autenticidad**: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.
- **Backup**: Se refiere a la copia de seguridad de los datos almacenados en un ordenador con el fin de que, en caso de algún problema informático que implique la pérdida de archivos, estos puedan ser recuperados **Base de datos:** es un conjunto de información que se relaciona entre sí, que está almacenada y organizada de forma sistemática para facilitar su preservación, búsqueda y uso.
- **Cifrar**: Transcribir en guarismos, letras o símbolos, de acuerdo con una clave; un mensaje o texto cuyo contenido se quiere proteger.
- **Confiabilidad**: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.
- **Confidencialidad**: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
- **Control**: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

- **Datacenter**: Se conoce también como centro de procesamiento de datos o centro de cómputo. Se refiere al espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
- **Disponibilidad**: Según [ISO IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.
- **Evento**: Según [ISO IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- **Firewall**: un cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas
- **Freeware**: es un programa informático cuya distribución es gratuita, por lo cual el usuario no tiene que pagar para instalarlo y utilizarlo.
- **FTP**: (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.
- **Impacto**: Resultado de un incidente de seguridad de la información.
- **Información**: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.
- **Ingeniería Social:** En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.
- **Integridad**: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- **IPS**: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.
- **ISO**: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
- **ISO 27001**: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

- **Keyloggers**: Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario.
- **Mail Bombing:** En el uso de Internet, una bomba de correo electrónico es una forma de abuso de la red que envía grandes volúmenes de correo electrónico a una dirección para desbordar el buzón.
- **Mail SPAM:** Los términos spam, correo basura, correo no deseado o correo no solicitado hacen referencia a los mensajes de correo electrónico no solicitados, no deseados o con remitente no conocido (o incluso correo anónimo o de falso remitente), habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.
- **Mail Spoofing:** Email spoofing es la creación de mensajes de correo electrónico con una dirección de remitente falso. Es fácil de hacer porque los protocolos básicos del servicio de correo electrónico no tienen ningún mecanismo de autenticación.
- **Mail Relay:** es un servicio web de email marketing. Es un software propietario para el envío de mailings, newsletters y análisis de campañas de correo electrónico.
- **Puertos USB**: El puerto USB o Universal Serial Bus (Bus Universal en Serie) es un puerto diseñado para conectar varios periféricos a una computadora
- **Seguridad perimetral informática** se refiere a la **seguridad** que afecta a la frontera de la red de nuestra empresa también llamada perímetro. Esta frontera o perímetro, está formada por el conjunto de máquinas y dispositivos que interactúan con el exterior, con otras redes.
- **Sistema Operativo**: Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.
- **SSID**: Un SSID (identificador de red SSID) es el nombre público de una red de área local inalámbrica (WLAN) que sirve para diferenciarla de otras redes inalámbricas en la zona. Para Google Fiber, SSID es el nombre de la red que se especifica al configurar la red Wi-Fi. Todos los dispositivos inalámbricos que se conectan a la red deben utilizar este SSID.
- **SOC**: Un Centro de Operaciones de Seguridad, es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet.
- **VPN**: significa "Virtual Private Network" (Red privada virtual) y describe la oportunidad de establecer una conexión protegida al utilizar redes públicas. Las VPN cifran su tráfico en internet y disfrazan su identidad en línea. Esto le dificulta a terceros el seguimiento de sus actividades en línea y el robo de datos.
- **WIFI**: es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos.

5. NORMATIVIDAD APLICABLE

- NTC-ISOIIEC 27001- 27002:2022: norma internacional para los sistemas de gestión de la seguridad de la información. (SGSI)

- Ley 1273 de 2009: Ley de protección de la información y de los datos
- Ley 1581 de 2012: Ley de protección de datos personales
- Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Ley 1266 de 2008: también conocida como Ley de Habeas Data, se aplica a todos los datos personales financieros, crediticios, comerciales y de servicios registrados en un banco de datos.

6. RESPONSABILIDAD

- Alta Dirección: La alta dirección de la OCBP, consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:
  - Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
  - Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
  - Impulsar la divulgación y la concienciación de la Política de Seguridad de la Información entre los empleados la organización.
  - Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
  - Considerar los riesgos de seguridad de la información en la toma de decisiones.

- Dirección de Sistemas: es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales, la estructuración, recomendación, seguimiento y mejora del Sistema en lo relacionado a seguridad de la información de la organización. Todo lo anterior con el apoyo del jefe de sistemas, coordinadores y del asesor de seguridad informática.

- Grupo responsable de Seguridad Informática: será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política. Este grupo está conformado por el jefe de sistemas, coordinadores y un técnico dedicado para labores de administración y monitoreo de las plataformas de seguridad informática.

- Los propietarios de activos de información (ver su definición en el glosario) son responsables de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

- El departamento de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula contractualmente con la Organización, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos sus procesos, procedimientos, prácticas y guías que surjan. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos o cláusulas de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados en la presente política.

- El departamento de Jurídica verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con

empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

- Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

- Empleados, terceros, contratistas: tiene la responsabilidad de cumplir con lo formalizado en este documento y aplicarlo en su entorno laboral. Además, tiene la obligación de alertar de manera oportuna y adecuada, según lo determine la política de manejo de incidentes, cualquier incidente que atente contra la seguridad de la información.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

La organización debe establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización:

- La alta gerencia debe brindar el apoyo y énfasis para la adecuada gestión de la seguridad de la información.

- La organización debe asignar el presupuesto para las actividades de seguridad y riesgo de la información.

- Debe existir un espacio definido para analizar el riesgo de la información, las políticas y los problemas de seguridad de la información.

- Los roles y las responsabilidades del proceso de seguridad de la información deben estar claramente definidos y asignados a personas adecuadamente capacitadas.

- Se deben mantener contactos apropiados con las autoridades pertinentes para las autoridades reguladoras u otras autoridades y organismos que podrían necesitar ser contactados en caso de consultas, incidentes y emergencias

- El personal encargado de la seguridad de la información debe mantener contacto regular, con grupos especiales de interés, foros y listas de correo profesionales en riesgo de la información y la seguridad.

- Se debe realizar el análisis de riesgo en la información en la gestión de proyectos, independientemente del tipo de proyecto.

8. POLITICA DE SEGURIDAD DEL RECURSO HUMANO

La organización debe establecer mecanismos para asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos para los roles para los que se consideran:

8.1. ANTES DE LA CONTRATACION:

- El área de Gestión Humana debe contar con un procedimiento documentado, implementado y evaluado para la selección de personal.

- Este procedimiento debe hacer contacto de referencias y verificación de los antecedentes de todos los candidatos a un empleo de a las leyes, reglamentaciones y ética pertinentes.

- Si el proceso de validación se subcontrata se deben revisar los procedimientos del proveedor a fin de que cumplan con lo establecido en la presente política.

- Para el caso de contratación de empleados con roles críticos en el manejo de información existen procesos de selección mejorados

8.2. DURANTE LA EJECUCION DEL CONTRATO

La organización debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización

- Debe existir un programa de cultura y educación sobre la seguridad de la información dirigido a todos los niveles de la organización incluyendo la alta gerencia.
- El contenido y las actividades de sensibilización de este programa de cultura y educación debe estar definido por el riesgo clave de información y los roles y responsabilidades asociados con la seguridad de la información.
- El programa de cultura y capacitación debe incluir exámenes y ejercicios periódicos para verificar el nivel de conocimiento así como acciones de seguimiento para cualquiera que tenga problemas en dichas pruebas.
- Es sumamente importante actualizar el contenido del programa de cultura y educación de la seguridad de la información teniendo en cuenta los riesgos de la información en evolución, las amenazas emergentes, las vulnerabilidades recientemente identificadas y los incidentes, y los cambios en la política de seguridad de la información.
- El personal de seguridad de la información y cualquier otro con funciones y responsabilidades específicas debe tener las competencias necesarias. La organización debe tener claros los requisitos de capacitación para ejercer estos cargos.
- La organización debe definir estrategias o un plan de comunicación para difundir temas de seguridad de la información. Estos canales pueden ser folletos, carteles, correos electrónicos, gestión de aprendizaje online, cuestionarios, concursos, videos, redes sociales, etc.

8.3. TERMINACION O CAMBIO DE EMPLEO

- Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado, contratistas y se deben hacer cumplir.
- Cuando una persona cambie de cargo o termine contrato se deben revisar los perfiles de usuario con el fin de que se garantice la confidencialidad de la información. Así mismo, se debe realizar la recuperación de los activos de información (documentos, datos, sistemas) que este funcionario tenía en su poder.

9. POLITICA DE GESTION DE LOS ACTIVOS DE LA ORGANIZACIÓN

Esta política busca la preservación de los activos de información como soporte del negocio.

9.1. RESPONSABILIDAD POR LOS ACTIVOS

- La organización debe identificar los activos asociados con información e instalaciones de procesamiento de información y se debe elaborar y mantener un inventario de estos activos.
- Los activos mantenidos en el inventario deben tener un propietario.
- Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo

9.1.1. USO ACEPTABLE DE LOS ACTIVOS

Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información

9.1.1.1. SISTEMA OPERATIVO

El sistema operativo es el entorno físico en el que se ejecuta la aplicación. Cualquier vulnerabilidad en el sistema operativo puede comprometer la seguridad de la aplicación. La protección del sistema operativo garantiza la estabilidad del entorno, el control del acceso a los recursos y el control del acceso externo al entorno.

- Los sistemas operativos, deben contar con los últimos parches de seguridad provistos por el fabricante debidamente aprobado e instalado, con el fin de dar el aseguramiento adecuado.
- Es sumamente importante que la versión del sistema operativo cuente con soporte del fabricante.
- Se debe otorgar a los usuarios permisos de sólo lectura para los directorios necesarios. Si los atacantes obtienen acceso a una aplicación, tendrán los permisos de usuario.
- Denegar el acceso de forma predeterminada.
- El acceso a los recursos se deniega a todos los usuarios excepto a los que se concede acceso explícitamente.
- Puede denegar los permisos de lectura y escritura para todas las estructuras de directorios a todos los usuarios. Sólo los usuarios a los que se otorgan estos permisos explícitamente tienen acceso a los directorios y archivos. Esta política también protege los recursos que un administrador ha pasado por alto.
- Se debe realizar mantenimiento preventivo al sistema operativo de los servidores y equipos de cómputo de acuerdo a lo establecido en el SIT-PA-004 MANTENIMIENTO PREVENTIVO Y CORRECTIVO y al SIT-IA-002 INSTRUCTIVO DE MONITOREO DE LOS SERVIDORES VIRTUALIZADOS
- Todos los equipos de cómputo deben estar vinculados al Directorio Activo con el dominio prevenir.com
- Se deben configurar los usuarios de acceso al sistema operativo con privilegios restringido. Solo el personal del departamento de Sistemas tendrá acceso a los equipos de cómputo como administradores; salvo excepciones que deben quedar debidamente documentadas y anexas al presente documento.
- El acceso a la configuración del sistema operativo de los servidores solo será permitido a los usuarios pertenecientes al grupo Administradores de Servidores.
- Se debe realizar backup periódico a los servidores de acuerdo a lo establecido en el procedimiento SIT-PA-001 PROCEDIMIENTO DE RESPALDO DE BASE DE DATOS y al instructivo SIT-IA-002 INSTRUCTIVO DE MONITOREO DE LOS SERVIDORES

VIRTUALIZADOS

- Se deben eliminar aplicaciones que no sean esenciales para reducir las posibles vulnerabilidades del sistema.
- Restrinja los servicios locales a los servicios necesarios para la operación.
- Los equipos de cómputos y servidores de la organización deberán ejecutar un Sistema Operativo autorizado por departamento de sistemas.
- Los equipos de cómputos deberán ser instalados y configurados únicamente por el personal de Sistemas o proveedores autorizado. Los usuarios no deberán instalar otro Sistema Operativo, remplazar al existente o generar un sistema de booteo múltiple. Tampoco deberán actualizar el Sistema Operativo existente, o instalar cualquier tipo de Software utilitario, juegos o programas.
- Los equipos deberán bloquearse luego de transcurridos un lapso razonable de tiempo con las facilidades que provee el sistema operativo o mediante el protector de pantalla.
- El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al usuario del grupo administrador.
- Es importante tener actualizados todos los otros programas que estén instalados en los pc y servidores como Navegadores web, plugins, lectores de PDF, Java, Flash Player, reproductores de audio y video, entre otros ya que cada día aparecen nuevas amenazas.

9.1.1.2. INTERNET

- El acceso a Internet e Intranet, es una herramienta de trabajo que provee la Institución a sus funcionarios, por lo tanto, es responsabilidad de cada usuario, utilizar prudente y apropiadamente este servicio.
- Todo evento que se dé a través del uso de este servicio, será administrado, monitoreado y regulado por el área de Sistemas el cual tendrá la potestad de realizar las acciones pertinentes en pro de la seguridad, confidencialidad, integridad y disponibilidad de los bienes informáticos y de la información de la OCBP, así mismo, reportará a al departamento de Gestión Humana y a Gerencia cualquier uso indebido del servicios, y se creará el Incidente de seguridad informática de requerirse a través de los mecanismos establecidos.
- Se prohíbe el acceso a sitios de Internet que no tengan relación alguna con los objetivos institucionales, tales como los relacionados con: sexo, racismo, apuestas, actividades criminales, drogas, juegos, y cualquier otra que se estime conveniente restringir, en relación al uso de buenas prácticas de la organización.
- Desde el Departamento de Sistemas se crearán y monitorearán perfiles de navegación con la finalidad de brindar a los usuarios medios de acceso y consulta a Internet. Estos perfiles dependen de la labor que realizara cada funcionario.
- La asignación de perfiles de navegación será previo análisis de necesidad y autorización del líder de área o proceso.
- El acceso a Internet está reservado para todos aquellos directivos, empleados, y terceros que lo requieran según sus funciones.
- No se autoriza a los funcionarios acceder a sitios para el establecimiento de charlas, salvo que tengan relación alguna con las funciones que desempeña. En caso de que el funcionario requiera charlas o intercambio de mensajes de texto, deberá hacer uso de los recursos brindados por la entidad.
- Sólo personal previamente autorizado podrá “descargar” información desde Internet (incluye software gratuito y de uso temporal), con fines investigativos, prueba, o de

apoyo en el desarrollo de actividades, test que se realizaran controladamente y bajo la supervisión y monitoreo del área encargada.

- Toda información descargada de Internet debe estar relacionada con los objetivos misionales, gerenciales y/o de apoyo de la OCBP y las funciones que lleva a cabo el usuario.
- Todos los archivos obtenidos de la red Internet deben ser revisados (filtrados) para detección de virus previo a ser descargados en cualquier computador, para ello debe estar instalado en todas los PC de la OCBP el antivirus Corporativo.
- El tiempo de acceso a Internet no debe interferir ni distraer a los usuarios de sus funciones normales.
- Prohibido crear conexiones compartidas de internet.
- No se puede realizar ningún tipo de compras, que no sean de uso de la organización con su respectivo permiso.
- Periódicamente se deben generar reportes que muestren entre otros: información acerca del nombre de sitios visitados, duración, estaciones desde las cuales se accedió al servicio y cualquier otra que se estime conveniente, cualquier anomalía deberá ser reportada al departamento de Gestión Humana y a la Gerencia.
- Prohibida la publicación de cualquier tipo de información perteneciente a la Organización en sitios personales u otros, sin la autorización correspondiente del propietario de dicha información.
- Obtención de acceso no autorizado sobre otras computadoras pertenecientes a cualquier otra organización o entidad.
- Instalación y uso de programas de tipo “peer-to-peer” para el intercambio de archivos en Internet (Ej. Kazaa, Morpheus, Limeware, emule, etc.)
- Se prestará el servicio de internet a usuarios y terceros, siempre que se encuentren presentes los requisitos de seguridad mínimos.
- Los usuarios solo podrán conectarse a internet usando los medios dispuestos por la institución y no podrán acceder a través de otros canales de proveedores de servicios de internet externo.
- La institución se reserva el derecho de restringir el acceso de los usuarios a ciertos sitios web, así como también la restricción parcial o total a internet de los mismos.

9.1.1.3. CORREO ELECTRONICO

- Solo las personas expresamente autorizadas por el líder de área pueden hacer uso del correo institucional.
- El servicio debe ser utilizado exclusivamente para temar relacionados con la función desempeñada.
- Los usuarios están sujetos a auditorias por parte del departamento de Sistemas en cuanto a tráfico y manejo seguro de la información enviada.
- El envío de mensajes a grupos o listas de destinatarios, funcionarios o externos, que no sean del ámbito de trabajo de funcionario que hace el envío, se encuentra prohibido. Se incluye en esta prohibición, el envío de mensajes conocidos como “cadenas”
- Está prohibido que los usuarios envíen alertas de seguridad. Si algún usuario recibe una alerta de seguridad debe reenviarla al departamento de sistemas, específicamente al correo ciberseguridad@organizacioncbp.org

- Se prohíbe expresamente, para todo usuario, el uso de técnicas de ataque a sistemas de correo electrónico como mail SPAM, mail Bombing, mail Spoofing, o mail Relay.
- Los usuarios tienen prohibido enviar o recibir mensajes electrónicos usando la identidad de otro usuario. Si fuera necesario leer el correo de alguien más (mientras un empleado se encuentre fuera o de vacaciones) el Líder de la respectiva área determinará a qué buzón deben ser redireccionados sus correos en su ausencia.
- Está prohibido enviar o reenviar mensajes, imágenes o videos que incluyan contenidos sexuales o que ofendan al tocar temas de género, nacionalidad, orientación sexual, raza, religión, orientación política o discapacidad.
- Está prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- Está prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.
- Está prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- Está prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.
- Prohibido abrir archivos adjuntos correos de dudosa procedencia. Notificar al departamento de sistemas de inmediato.

9.2. CLASIFICACION DE LA INFORMACION

- La información se debe clasificar en función de los requisitos legales, valor criticidad y susceptibilidad a divulgación o a modificación no autorizada
- Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización
- Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización

9.3. POLITICA DE MANEJO DE MEDIOS

Esta política se aplica para la protección de los medios de almacenamiento removibles tales como: Memorias USB, discos externos, CD y DVD, discos duros externos, cintas de almacenamiento para Backups, que sean entregados por la Organización para manejo de la información; activos de información, que se encuentren clasificados dentro su inventario o cualquier tipo de sistema que permita el almacenamiento de datos, y sea utilizado para almacenar, administrar o transportar información de la OCBP. Así como para el manejo del borrado seguro y disposición de medios.

- La entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por la OCBP, velando por la disponibilidad y confidencialidad de la información.
- Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.
- En los casos en los que se almacene información en las pantallas y equipos que se encuentran en las salas de reuniones de la Entidad, salas de juntas y salones de

capacitación; las personas que han realizado la reunión, en el momento que no se requiera su uso en estos dispositivos, deben eliminarla de forma permanente; con el fin de evitar que personas no autorizadas puedan conocerla.

- Se debe contar con un registro de activos completo y actualizado de CD / DVD, almacenamiento USB y otros medios extraíbles.

9.3.1. GESTION DE MEDIOS REMOVIBLES

- El departamento de Sistemas debe disponer de los medios y equipos requeridos por los funcionarios para realizar sus labores. Así mismo, debe aplicar medidas de protección en la utilización de dichos medios, así como autorizar el formateo de discos externos y memorias USB a solicitud del usuario.
- El usuario que utiliza los medios removibles asignados es responsable de la custodia de la información y de velar por la integridad de la información que protegen.
- El Proveedor que recibe la información es responsable de velar por la protección e integridad de la información que salvaguarda.
- Ningún medio removible debe ser utilizado como alternativa de respaldo de la información de la OCBP, siendo responsabilidad de los usuarios mantener la información en los servidores y repositorios destinados para ello. Excepto en los casos autorizados por la Alta Gerencia o la Dirección o Jefatura de Sistemas.
- El uso de medios de almacenamiento removibles está restringido en la OCBP, excepto para aquellos funcionarios o terceros que sean autorizados por parte del líder de área y el área de sistemas para el desarrollo de sus labores.
- La solicitud para el uso del medio removible debe ser solicitado formalmente al técnico de seguridad informática, quien estudia, evalúa y autoriza la entrega de este, la cual debe ser registrada, según lo establecido en esta política.
- Se mantendrá un registro sobre las personas autorizadas al uso de medios de almacenamiento removibles.
- Es responsabilidad exclusiva del usuario del medio removible (funcionario, contratista, proveedor) tomar las medidas necesarias para el almacenamiento y resguardo de los medios removibles, para evitar accesos no autorizados, daños, pérdida de información o extravío de estos.
- La OCBP con apoyo del área de sistemas proporcionará las soluciones tecnológicas que permitan el monitoreo, verificación de presencia de programa maligno (Malware) y control de los medios de almacenamiento removibles.
- La información que se encuentre en los medios de almacenamiento deberá ser borrada de forma segura; si ya no es requerida para el soporte de funciones de la OCBP.
- Todo medio de almacenamiento que sea propiedad de la OCBP y que quiera ser retirado de sus instalaciones deberá ser notificado por el usuario respectivo para proceder con la respectiva autorización.
- Los medios de almacenamiento deberán ser almacenados en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes y proveedores.
- Cuando la información que se encuentra almacenada en un medio removible de propiedad de la OCBP pierda vigencia, se debe formatear o destruir el medio de forma segura.
- El técnico de seguridad informática definirá los procedimientos de notificación en caso de pérdida de los dispositivos de almacenamiento removible. Si el caso relaciona un dispositivo de almacenamiento que no era propiedad de la OCBP pero que contenía información de la entidad, deberá notificarse como incidente de seguridad de la información a través del respectivo procedimiento.

- Las personas autorizadas antes de abrir cualquier elemento que se encuentre dentro del dispositivo de almacenamiento deben ejecutar el antivirus sobre éste, con el objetivo de evitar infecciones en su estación de trabajo.

9.3.2. TRANSFERENCIA DE INFORMACION

- Cualquier tipo de información de uso, no debe ser transferida a terceros sin que medie autorización superior o un compromiso de confidencialidad entre la OCBP y el tercero.
- Toda información que se genere procese, almacene y/o transite por la red de la organización se considera propiedad de OCBP.
- La información transmitida, procesada producto de las funciones del personal y que concierne a la OCBP o a sus usuarios, no podrá ser interceptada o divulgada bajo ninguna circunstancia, por ningún usuario interno de la OCBP, salvo en aquellos casos que los organismos de control establezcan bajo órdenes judiciales.
- Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte
- Se debe emplear un mecanismo de cifrado adecuado durante el proceso de transferencia.
- Se debe dejar constancia de la recepción por el destino durante el proceso de transferencia (Acta, Email, Certificación de mensajería, etc.)

10. POLITICA DE CONTROL DE ACCESO

La organización debe definir lineamientos y mecanismos para limitar el acceso a la información y a instalaciones de procesamiento de información.

10.1. SEGURIDAD FISICA Y DEL ENTORNO: proteger físicamente la información y controlar el acceso físico.

- Se debe tener acceso controlado y restringido a los lugares sensibles donde se maneja información: Archivo principal, Datacenter, cuartos de comunicaciones. Solo el personal autorizado por la oficina de Sistemas y de archivo puede ingresar a estos sitios.
- Para los sitios antes mencionados debe quedar un registro un registro de todas las entradas y salidas.
- Los puntos de acceso tales como áreas de carga, despacho, recepción u otros puntos que podrían permitir el acceso a personas no autorizadas deben ser controlados y, si es posible, aislados de las instalaciones de procesamiento de información para evitar accesos no autorizados.
- Los espacios físicos donde se ubiquen los servidores, rack de comunicaciones deberán estar protegidos adecuadamente mediante controles de acceso perimetrales, sistemas de vigilancia y medidas preventivas de manera que puedan evitarse o mitigar el impacto de incidentes de Seguridad (accesos no autorizados a sistemas de información, robo o sabotaje). Adicionalmente, el techo exterior, las paredes y el suelo son deben ser de construcción sólida.
- Se prohíbe el ingreso de personas a cualquiera de las instalaciones físicas mencionadas anteriormente, bajo estas condiciones:
  - En estado de embriaguez o bajo la influencia de narcóticos o drogas enervantes
  - Portando cámaras fotográficas y filmadoras.
  - Fumando

- El archivo y el Datacenter deben ser mantenidos en un ambiente seguro y protegido por los menos con:
  - Detección de incendio y sistemas de extinción de conflagraciones.

- Controles de humedad y temperatura.
- Bajo riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

- Los sistemas de control de temperatura, respaldo eléctrico, control de incendio, control de acceso deben estar cubiertos por mantenimiento preventivo y correctivo.

- La oficina de archivo debe realizar periódicamente un saneamiento ambiental con el fin de conservar los documentos. Este proceso debe incluir labores de limpieza, desinfección, desinsectación y desratización, para controlar el material particulado, suciedad y agentes bióticos en las instalaciones físicas de archivo.

- Los servidores, la red de Datos y equipos de cómputo deben estar cubierta por mantenimiento y soporte adecuados de hardware y software.

- Los equipos portátiles deben estar correctamente aseguradas y operadas por personal de la institución.

- Los equipos de cómputo no se deben retirar del sitio sin autorización previa.

10.2. **GESTION DE ACCESO A USUARIOS:** Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. El acceso a los recursos de tecnologías de información institucionales debe estar restringidos según los perfiles de usuario.

- La asignación de la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información

- La concesión de esos privilegios solamente por el tiempo que sea necesario para el desarrollo de las tareas

- Se deberán establecer procedimientos y mecanismos que aseguren la confidencialidad de la información secreta de autenticación para los usuarios genéricos de administración (por ejemplo, modificación frecuente de contraseña, mecanismos de compartición de la contraseña seguros, etc.).

- El acceso a la base de datos solo está autorizado al personal que lo requiera. Este acceso debe ser solo de consulta. Solo el administrador de la base de datos está autorizado para ingresar con todos los privilegios a la Base de Datos.

- El departamento de sistemas debe elaborar, mantener y publicar procedimientos de administración de cuentas de usuario para el uso de servicios de red.

- La OCBP debe propender por mantener al mínimo la cantidad de cuentas de usuario que el personal, terceros y auditores deben poseer para acceder a los servicios de red.

- Las claves de administrador de los sistemas deben ser conservadas por la dirección de la OCBP y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

- Como requisito para la terminación de relación contractual - o laboral - del personal de la OCBP debe existir un procedimiento de cancelación de las cuentas de usuario asignadas para el uso de recursos de tecnologías de la información de la organización.

- Las cuentas de usuario deben ser solicitadas por el líder del área al departamento de Sistemas a través del PQRS.

- Las cuentas de usuarios, contraseñas o cualquier otro mecanismo de autenticación a los sistemas de información, deben ser tratadas como información confidencial de la Institución, por lo cual no se deben divulgar, publicar ni compartir con ninguna persona.

- Las credenciales de acceso a los sistemas operativos, aplicaciones o a la red no podrán ser almacenadas sin cifrar, en cualquier medio físico, magnético o electrónico.

- Toda transacción y actividad realizada con la cuenta de usuario asignada a los sistemas de información de la Institución, es responsabilidad del propietario de dicha cuenta.

- Las contraseñas o cualquier otro método de autenticación a la red administrativa deben mantenerse bajo reserva y ser entregadas de forma personal o a través de un medio que asegure su confidencialidad.

- La asignación de información de autenticación secreta, se debe controlar mediante un proceso de gestión formal que incluya:
    - Controles técnicos como la longitud mínima de la contraseña, reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc.), cambio forzado de contraseñas en el primer uso, autenticación de múltiples factores, datos biométricos, contraseñas compartidas etc.
    - Evitar la reutilización de un número específico de contraseñas.
    - Contraseñas cifradas
    - Confirmación de la identidad de los usuarios antes de proporcionarles contraseñas temporales nuevas.
    - Generación de contraseñas temporales lo suficientemente fuertes
    - Almacenamiento de forma cifrada las contraseñas en sistemas, dispositivos y aplicaciones.

- El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el personal de Sistemas, que contengan información que pueda facilitar a un tercero la obtención de la información de su usuario de acceso.

- Los usuarios, tanto internos como terceros, darán un seguimiento estricto sobre las políticas de creación de contraseñas, acatando sus disposiciones en su totalidad.

- Se consideran usuarios externos o terceros cualquier entidad o persona natural que tenga una relación con la OCBP fuera del ámbito empleado/Contratista y siempre que tenga una vinculación con los servicios de la organización.

- El acceso a la red por parte de terceros es estrictamente restrictivo, éstos tendrán acceso únicamente a los servicios de Internet y recursos públicos compartidos de la red y permisible mediante firma impresa y documentación de aceptación de confidencialidad de la Organización, comprometiéndose con el uso exclusivo del servicio para los fines que fue provisto el acceso.

- La solicitud y los permisos de acceso de los terceros dependerá de la finalidad del acceso y en lo posible a través de conexiones VPN
    - El acceso por parte de terceros es temporal y debe ser solicitado al área de Sistemas por el funcionario de la organización que este acompañando al proveedor, cliente o ente de control. Esta conexión se realiza a través de la Wifi pública la cual solo permite acceso a internet restringido.
    - No se proporcionará el servicio solicitado por un usuario, o área de trabajo, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.

- Se debe hacer una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones de acuerdo.
- Se deben realizar revisiones más frecuentes y periódicas de cuentas privilegiadas para identificar y deshabilitar / eliminar cuentas con privilegios redundantes y / o reducir los privilegios.
- El no cumplimiento de las disposiciones de seguridad y responsabilidad sobre sus acciones por parte de los usuarios de la red institucional se obliga a la suspensión de su cuenta de usuarios de servicios.

10.3. ACCESO A REDES Y SERVICIOS DE RED

Consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de la red informática de la OCBP y los recursos accesibles:

- Son usuarios de la red institucional los empleados de planta, administrativos, contratistas y toda aquella persona que tenga contacto directo y utilice los servicios de la red institucional de la OCBP.
- El Departamento de Sistemas diseñará los mecanismos necesarios para proveer acceso a los servicios de la red institucional.
- Se deben implementar mecanismos que garanticen la seguridad perimetral de la red que permitan bloquear el acceso no autorizado, y determinar que qué datos, voz y vídeo pueden entrar y salir de la red.
- El departamento de Sistemas deberá emplear dispositivos de red para el bloqueo, enrutamiento y/o filtrado del tráfico, evitando el acceso o flujo de información no autorizado, hacia la red interna o desde la red interna hacia el exterior.
- Está estrictamente prohibido a los empleados y terceros que tengan acceso a red inalámbrica o cableada, menoscabar o eludir los controles establecidos por la Institución para la protección de los activos de información.
- Los sistemas de comunicación tales como routers, switch, AP, entre otros dispuestos para el servicio de OCBP, son los únicos autorizados para su uso en la red y solo pueden ser administrados por el personal técnico el departamento de Sistemas o proveedores autorizados.
- El acceso a la red interna se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido mediante un mecanismo de autenticación (usuario de dominio de manera preferencial, salvo en casos específicos y debidamente autorizados)
- En la red administrativa no está permitido hacer uso de los recursos para acceder a redes sociales, servicios interactivos de almacenamiento masivo, streaming de entretenimiento, páginas de mensajería instantánea sin previa autorización.
- Cualquier tipo de ataque, así como efectuar un escaneo, prueba o penetración de sistemas de computación, redes en Internet, o redes internas, está estrictamente prohibido, salvo en casos debidamente autorizados por la Dirección de Tecnología de la información y por requisitos propios de la Institución.
- Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado una auditoría de seguridad.
- Los accesos a la red interna o local desde una red externa de la Organización o extranet se harán mediante unos mecanismos fuertes de autenticación.
- Se registrará todo acceso a los dispositivos de red mediante archivos de registro o logs, de los dispositivos que provean estos accesos

- Los mecanismos de autenticación y permisos de acceso a la red, deberán ser evaluado y aprobados por el Departamento de Sistemas.
- El personal de soporte o administración que requiera acceder remotamente a la red de datos institucional lo debe hacer preferiblemente desde los portátiles corporativos o desde un computador personal en caso de no disponer de un corporativo, en ningún momento lo hará desde una red o área de servicios públicos.
- Es totalmente prohibido, salvo autorización o supervisión expresa del Departamento de Sistemas, la intervención física de los usuarios sobre los recursos de la red institucional (cables, enlaces, estaciones de trabajo, equipos de red, etc.).
- Los usuarios deben evitar el uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WiFi, Bluetooth, o infrarrojos en los dispositivos móviles asignados.
- Todas las conexiones que se originan desde redes o equipos externos hacia la OCBP, deben limitarse únicamente a los servidores y aplicaciones necesarias. Si es posible, estos servidores destino de las conexiones deben estar físicamente o lógicamente separados de la red interna de la entidad por medio de una zona desmilitarizada (DMZ).
- Las conexiones remotas hacia la red de la OCBP deben hacerse a través de VPN. Las excepciones deben autorizarse por el departamento de sistemas.

10.3.1. ACCESO A REDES Y SERVICIOS DE RED

Las redes inalámbricas requieren de un alto grado de responsabilidad por parte de los usuarios de la red para aprovechar y maximizar los beneficios de la tecnología, brindando cobertura de red inalámbrica y un sistema de comunicaciones seguro en las edificaciones de la entidad.

- Los equipos y antenas inalámbricas única y exclusivamente deberán ser instalados por personal de sistemas de la OCBP, o por quien se autorice para su instalación y destino de utilización.
- Los usuarios deberán evitar el mal uso de la red inalámbrica de la OCBP, como el acceso a sistemas o aplicaciones no autorizadas (Redes Sociales, reproducción de videos, juegos en línea, descarga de aplicativos) que afectan el desempeño de la red inalámbrica diseñada y destinada con fines netamente laborales, para aplicativos misionales y de apoyo y paginas corporativas de aplicaciones de la entidad.
- Se restringe la propagación de SSID de dispositivos de anclaje, como modem 3G, 4G, y zonas de anclaje de celulares Smartphone.

10.4. ACCESO A SISTEMAS Y APLICACIONES

- El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
- El acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro de tal manera que:
  - Se informe el acceso no autorizado
  - Se autentiquen las identidades de usuario durante el proceso de inicio de sesión
  - Las contraseñas no válidas desencadenan bloqueos
  - Se registran los inicios de sesión exitosos
  - Se transmiten las contraseñas de modo seguro mediante el uso de cifrado
- Se debe restringir el acceso a los códigos fuente de los programas
- Se debe controlar los accesos privilegiados a través de un proceso formal que restrinja y audite este tipo de accesos.

11. POLITICA DE DISPOSITIVOS MOVILES

Esta política define las condiciones para el manejo de los dispositivos móviles institucionales o personales que acceden a información de la OCBP, y vela por el uso responsable de estos por parte del personal.

- Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, el departamento de sistemas debe implementar:
  - Controles de acceso
  - Técnicas criptográficas para cifrar la información crítica almacenada en estos
  - Mecanismos de respaldo de la información que contienen
- El personal que haga uso del dispositivo móvil para almacenar o acceder a la información de la OCBP, deberá:
  - Aceptar las configuraciones de seguridad del dispositivo por medio de correo electrónico, y estas no podrán modificarse mientras se acceda o almacene información de la OCBP.
  - Está prohibido almacenar información personal en los dispositivos móviles asignados por la OCBP.
  - Está prohibido realizar instalación de aplicaciones no autorizadas por el departamento de Sistemas.
  - Para aquellos dispositivos que no son entregados por la OCBP, deben aceptar por escrito el cumplimiento la política de dispositivos móviles, así como las configuraciones de seguridad establecidas.
  - En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de la OCBP, se debe reportar la perdida al departamento de Sistemas lo más pronto posible.

12. CONTROLES CRIPTOGRAFICOS

Los controles criptográficos están enfocados a la protección de la información en el caso de que un intruso pueda tener acceso físico a la información, se impone establecer un sistema de cifrado de la misma para dificultar la violación de su confidencialidad o su integridad.

- Se debe implementar claves criptográficas en los dispositivos móviles: portátiles y tabletas.
- La gestión de claves debe realizarse de tal manera que se garantice la correcta generación, uso y protección, distribución, renovación o destrucción.
- Los usuarios de las claves criptográficas aceptan el manejo confidencial de las mismas.

13. POLITICA DE SEGURIDAD EN LAS OPERACIONES

Estos controles buscan que las operaciones de tecnologías de la información se hagan de manera correcta y segura.

13.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.

13.1.1. PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS

- Las operaciones de tecnologías de información, sistemas y gestión de redes, gestión de incidencias, la administración y seguridad de tecnologías de información, seguridad física, gestión de cambios, entre otros deben estar debidamente documentados.
- Estos procedimientos deben ser razonablemente seguros y están siendo revisados y mantenidos rutinariamente, autorizados, compartidos y usados.

- Los roles y responsabilidades deben estar bien definidos y se debe capacitar adecuadamente al personal.

13.1.2. GESTION DE CAMBIO

Se deben establecer, coordinar, controlar y documentar los cambios realizados en los activos de información tecnológicos y los recursos informáticos, asegurando que los cambios efectuados sobre la plataforma tecnológica hayan sido debidamente autorizados por las áreas correspondientes. Por tanto:

- Los cambios a nivel de tecnologías de información deben quedar registros de tal manera que se cuente con información de:
  - Quien autoriza los cambios
  - Quien realiza los cambios
  - Fecha
  - Descripción de las tareas
  - Validación del cambio
- Los cambios deben ser planificados y deben estar acompañados de pruebas realizadas y comunicaciones a todos los involucrados.
- Los cambios deben estar debidamente evaluados, documentados, justificados y autorizados por la dirección de Sistemas y en algunos casos, de acuerdo a la criticidad, por la Dirección de operación o la Gerencia.
- Se deben establecer pautas para implementar cambios de emergencia.
- El departamento de Sistemas debe garantizar que todo cambio realizado a un componente de la plataforma tecnológica, el cual conlleve modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes.
- El departamento de Sistemas debe garantizar que todo cambio realizado sobre la plataforma tecnológica de la Organización quedará formalmente documentado desde su solicitud hasta su implantación cumpliendo con el procedimiento correspondiente.
- Se deben establecer líneas base de configuración de la plataforma tecnológica, que permitan llevar la trazabilidad de los cambios.
- Los propietarios de los activos deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.
- El departamento de TI debe garantizar que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios, siguiendo los procedimientos vigentes para dicha acción

13.1.3. GESTION DE LA CAPACIDAD

Se debe monitorear e identificar el uso de recursos de infraestructura tecnológica que permita realizar proyecciones sobre la capacidad asegurando el óptimo desempeño de los servicios, aplicaciones y sistemas de información de la organización. Se debe:

- Alinear la gestión de capacidad al plan estratégico de TI.
- Medir y hacer seguimiento a recursos de TI como servidores, equipos de cómputo, impresoras, base de datos, internet, redes, etc.
- Controlar el rendimiento de la infraestructura TI.
- Asegurar que se cubren las necesidades de capacidad TI tanto presentes como futuras.

- Desarrollar planes de capacidad asociados a los niveles de servicio acordados.
- Planificar las ampliaciones de capacidad de los recursos cuando sea necesario.
- Gestionar y racionalizar la demanda de servicios TI.
- Optimizar el uso de recursos.

13.1.4. SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN

Se deben definir las directrices para la separación de los ambientes de desarrollo, prueba y producción en la generación de software o aplicaciones internas para reducir los riesgos de acceso no autorizado o cambios en el sistema operacional.

- Se deben separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
- Se debe contar con acceso a través de perfiles de usuario debidamente diferenciados para cada uno de estos entornos.
- Durante la fase de desarrollo de la aplicación se deberá documentar y archivar todos los modelos de la aplicación (procesos funcionales, datos, prototipos, casos de uso, de secuencia, de estado, etc.) que se haya derivado de la fase de requerimientos y diseño de la aplicación.
- Durante la fase de desarrollo se deberá disponer de un ambiente especializado para estos fines, el que debe ser totalmente independiente respecto al que se utilice posteriormente para pruebas, capacitación y/o producción. Este ambiente debe asegurar el correcto funcionamiento de todas las herramientas necesarias para esta fase (editores de código fuente, compiladores, etc.) y que no deben quedar disponibles en la fase de producción.
- Las pruebas de usuario no deben hacerse en el computador personal del desarrollador, debe hacerse en un entorno definido para tal fin. Este ambiente no debe ser utilizado para actividades de desarrollo o producción.
- El ambiente de pruebas no debe poseer herramientas de software o permisos de acceso especiales para ejecutar desarrollos de software, en su lugar debe tener una configuración similar o igual a los de producción.
- Una versión se instala en producción solo después que ha sido instalada y probada en ambiente de pruebas y los líderes responsables de procesos den su visto bueno.

13.2. PROTECCION CONTRA CODIGO MALICIOSO

Se deben implementar controles de detección, de prevención y de recuperación combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos.

El software malicioso, también conocido como programa malicioso o malware, contiene virus, spyware y otros programas indeseados que se instalan en su computadora, teléfono o aparato móvil sin su consentimiento. Para evitar esto se debe:

- Los servidores, al igual que todas las estaciones de trabajo tendrán instalado y correctamente configurado (con agente de red apuntando a servidor consola de antivirus) software antivirus y activada la protección en tiempo real.
- El encargado de Administrar la Infraestructura de la organización, en conjunto con el Coordinador de Soporte Técnico, supervisarán la instalación y correcta configuración del software antivirus en todas las estaciones de trabajo. Para los servidores la instalación y configuración será supervisada por el administrador de infraestructura.

- Sin importar el origen del software y la utilización del mismo, ninguna clase de archivo ejecutable será puesto en marcha sin antes haber pasado el control de análisis sobre la seguridad del mismo.
- No se debe instalar ninguna aplicación y menos desde internet. Si requiere alguna aplicación en particular debe solicitarlo al área de Sistemas puesto que son los únicos autorizados para esta tarea.
- No se debe entrar en los enlaces que te envíen ni descargues los adjuntos de los correos electrónicos.
- Evita dar información personal cuando se navegue por Internet.
- Evitar la descarga de archivos. Cuando se requiera por temas laborales, debe realizarse desde sitios seguros accediendo a sitos web oficiales y previa consulta al área de tecnología de información.
- Utilizar una conexión segura. La conexión debe realizarse a través de HTTPS (Hipertext Transfer Protocol Secure). Al acceder a una página web a utilizando este protocolo, la comunicación entre el cliente y el servidor viaja cifrada, lo que aumenta la seguridad y minimiza la posibilidad del robo de contraseñas.
- Evitar los enlaces engañosos. No abrir correos de dudosa procedencia, idiomas distintos al español, correos de una entidad bancaria para actualizar la información, cadenas de correo acerca del cambio de un servicio de correos gratuito a pago o un multimillonario que quiere regalar su dinero.

13.3. COPIAS DE RESPLADO

Se deben hacer copias de respaldo de la información, software o imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con la política de copias de respaldo acordadas:

- Toda la información confidencial y sensible que está alojada en las plataformas tecnológicas de la OCBP debe ser salvaguardada de manera sistemática y periódica.
- El área de Sistemas debe garantizar el cumplimiento de la copia de seguridad de la base de datos y de los servidores, de acuerdo a lo establecido en el procedimiento de respaldo de servidores y base de datos.
- Será responsabilidad de cada usuario realizar el respaldo de su información, así como de cada Jefatura de los archivos que sean de uso común para el desarrollo de sus actividades misionales, de acuerdo a lo establecido.
- La ubicación de los medios de almacenamiento deberá estar alejada del polvo, humedad, o cualquier contacto con material o químicos corrosibles.
- Se debe tener en cuenta el mantenimiento en perfecto estado de funcionamiento de los medios que nos permitirán la restauración de las copias cuando se necesiten.
- Los medios de recuperación y el sistema de copias de seguridad deben permitir restauraciones parciales del sistema dependiendo de las distintas aplicaciones y sistemas de forma que un incidente de corrupción de un sistema o aplicación no obligue a la restauración de otras aplicaciones con el consiguiente impacto

13.4. REGISTRO Y SEGUIMIENTO

Los sistemas de información deben mantener registros que a su vez deben ser monitoreados y auditados. Por tanto:

- Se debe mantener un registro de los eventos que, ante un incidente, permitan determinar qué estaba sucediendo mediante los datos de la hora, la fecha del incidente, etc., las personas involucradas, el origen y las causas, etc.
- Se debe revisar los registros de forma periódica, independientemente de si hay un incidente o no. Esto puede ayudar a analizar tendencias, detectar potenciales actividades fraudulentas, o detectar el origen de fallos de funcionamiento, antes de que ocurran incidentes importantes.
- Los registros de eventos deben tener el nivel de protección apropiado para evitar pérdidas, corrupción o cambios no autorizados y donde sea posible, nadie debe tener permiso para borrar o desactivar el registro de sus propias actividades.
- Se deben guardar copias de seguridad de los registros de eventos.
- Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.

13.5. CONTROL DEL SOFTWARE OPERACIONAL

Las incompatibilidades en instalaciones de nuevo software o en actualizaciones de versiones existentes pueden afectar tanto al funcionamiento del propio software o aplicación como al rendimiento de los equipos y afectar de rebote a otros sistemas o aplicaciones. Por tal razón se deben implementar controles que eviten tal situación:

- Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
- Probar las nuevas aplicaciones o software en entornos aislados especialmente preparados para pruebas.
- Comprobar las necesidades de instalación (compatibilidad del entorno) antes de su instalación.
- Valorar la necesidad de actualización o instalación.
- Planificar la forma de volver a versiones anteriores en caso de ser necesario.

13.6. GESTION DE VULNERABILIDADES TECNICAS

Actualmente todas las aplicaciones software están sujetas a actualizaciones con propósito de mejorar no solo su funcionalidad sino sobre todo la seguridad de las mismas. Se debe gestionar posibles vulnerabilidades:

- Identificar posibles debilidades técnicas mediante la consulta de foros especializados,
- Mantener actualizada la información de fabricantes y proveedores
- Realizar pruebas de ataques simulados (hacking ético)
- Escaneos periódicos de vulnerabilidades

14. POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES

Puesto que los intercambios de información se realizan a través de redes de comunicaciones se deben establecer los controles adecuados para proteger tanto las comunicaciones externas a la organización como las que viajan a través de las redes de la propia organización.

14.1. GESTIÓN DE LA SEGURIDAD DE LAS REDES

- Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
- Se deben asignar responsabilidades dentro del equipo de gestión y que se siguen una serie de procedimientos establecidos.
- Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
- Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
- Cuando la información se transfiere a través de redes públicas o redes inalámbricas, se deben considerar controles adicionales para mantener las conexiones (disponibilidad) y la privacidad (confidencialidad) y la integridad de los datos.

14.2. TRANSFERENCIA DE INFORMACIÓN

Se trata de requisitos o controles para proteger la información cuando se transmiten datos bien sea internamente o entre varias entidades.

- Se debe contar con política, procedimientos y controles de transferencia de información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
- Los acuerdos deben tratar la transferencia segura de la información del negocio entre la organización y las partes externas.
- Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
- Se deben establecer acuerdos de confidencialidad tanto a personal propio como a clientes y proveedores si tiene acceso a activos de información que así lo requieran.

15. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La organización debe implementar controles para la seguridad de la información al ciclo de vida completo de los sistemas de información, tanto propios como subcontratados.

15.1. SEGURIDAD EN LOS SISTEMAS DE INFORMACION

La seguridad de los sistemas de información se refiere al proceso de desarrollar, añadir y probar características de seguridad dentro de las aplicaciones para evitar vulnerabilidades de seguridad contra amenazas, tales como la modificación y el acceso no autorizados.

Garantizar que la seguridad de la información es una parte integral de los sistemas de información en todo su ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios través de las redes (privadas y públicas).

- Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
- La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se deben proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
- La información involucrada en transacciones de los servicios de aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y duplicación o reproducción de mensajes no autorizada.

15.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

Se debe garantizar que la seguridad de la información ha sido diseñada e implementada dentro del ciclo de vida del desarrollo de los de los sistemas de la información:

- Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
- Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
- Cuando se cambian plataformas de operación se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
- Se debe limitar los cambios en los paquetes software para minimizar la posibilidad de generar incidentes. Se debe limitar las actuaciones sobre el software a cambios absolutamente necesarios.
- Se debe implementar un ambiente de desarrollo seguro. La evaluación de riesgos para la seguridad de la información no solo debe afectar a los activos de información como software, datos o equipos y soportes sino que también debe aplicarse a los entornos de desarrollo, las personas, los procesos de desarrollo y las tecnologías utiliza dadas para determinar si es necesario aplicar medidas o controles de seguridad. Por tanto se debe tener en cuenta:
    - El grado de sensibilidad de los datos
    - Los niveles de seguridad aplicables
    - La confiabilidad del personal
    - Las necesidades de separar entornos de desarrollo
    - Los controles de acceso determinados para el entorno de desarrollo
    - Las necesidades de respaldo de la información.
- En el caso del desarrollo de software subcontratado se debe:
    - Establecer y supervisar el cumplimiento de los requisitos de seguridad
    - Controlar y gestionar todos los aspectos de licencias y propiedades de código fuente
    - Metodología y definición de las pruebas a realizar al software subcontratado
    - Todo lo anterior debe ser plasmado en acuerdos firmados y consensuados con el proveedor
- Los requisitos para la seguridad de un sistema software deben ser probados como si se tratase de una funcionalidad más del software. Para ello debería implementarse un plan de pruebas documentado.
- El proceso de incorporación de nuevas aplicaciones actualizaciones o nuevas versiones de software debe estar sujeto a un proceso de aceptación donde se le realicen las pruebas funcionales y de seguridad planificadas.

15.3. DATOS DE PRUEBA

Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente. Para ello se pueden utilizar alternativas como:

- Utilizar datos no reales para los desarrollos y pruebas posteriores de los sistemas.
- Enmascaramiento de datos.
- En caso de que esto no fuera posible se deben aplicar los mismos controles de seguridad (acuerdos de confidencialidad etc.) que se aplican a los datos reales.

16. RELACIONES CON PROVEEDORES

Se deben establecer las directrices y los requisitos de seguridad de la información entre la Organización Clínica Bonnadona Prevenir y sus proveedores o terceros. En especial aquellos que tengan acceso a los sistemas de información o a los recursos que manejan activos de información.

Acuerdos con los proveedores:

- Estas directrices deben contemplarse antes, durante y a la finalización del contrato o servicio.
- Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar entre éstos y se deben documentar.
- Se deben definir e implementar contratos y acuerdos de seguridad de información con los proveedores. Estos acuerdos deben incluir:
    - Descripción de la información que se maneja y el método de acceder a dicha información
    - Estructura de la clasificación de la información a usar
    - La Inmediata notificación de incidentes de seguridad
    - Subcontratación y restricciones en las relaciones con otros proveedores
    - Responsabilidades relacionadas con el riesgo y la seguridad de la información
    - Control de personal
    - Requisitos legales y normativos
    - Correcto uso de activos de información
    - Derecho de monitoreo y/o auditoría de seguridad por parte de la organización para cumplir con los requisitos de seguridad
    - Cumplimiento de procesos de seguridad por parte del proveedor y/o tercero
    - Identificación de controles físicos y lógicos
    - OCBP tendrá actualizada la información correspondiente de la persona de contacto de los proveedores.

Adquisiciones:

- Para toda adquisición de software y hardware que OCBP realiza, es responsabilidad del proceso de Sistemas definir los requisitos de seguridad, de acuerdo al procedimiento de compras.
- Los proveedores que estén relacionados con el suministro de tecnología de información y comunicación que prestan a OCBP, deben asegurar que los requisitos y buenas prácticas de seguridad implementadas por OCBP sean extensivos a sus terceros que intervengan directamente con los servicios prestados a OCBP.

Seguimiento a los proveedores:

- Se establece llevar a cabo el seguimiento periódico de conformidad al procedimiento de compras, considerando el tipo de proveedor, acuerdos de niveles de servicio y criticidad de la información que maneja.
- En caso de ser requerido por norma o Ley, o en aquellos casos que OCBP considere pertinente, se ejecutaran auditorías de tercera parte a los proveedores.
- 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.

- Los empleados de OCBP que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas, así mismo, deberán acogerse a las recomendaciones que se emitan como resultado de las auditorias que realicen sobre los mismos.

17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad de la información reportados en la organización deben gestionarse adecuadamente. De tal manera que exista un marco para la identificación, clasificación, respuesta y análisis de incidentes de seguridad de la información, garantizando la continuidad del negocio, la protección de la información y la mejora continua de los controles de seguridad. Para ello:

- La Organización debe contar con herramientas, procesos y personal experto que permitan la identificación y tratamientos de amenazas.
- Los incidentes de seguridad, inquietudes, observaciones, deben ser reportados al correo ciberseguridad@bonnado.co
- Los incidentes de seguridad se deben clasificar de acuerdo al impacto y categorizarlos de acuerdo a la naturaleza.
- Todo incidente de seguridad debe ser analizado detalladamente y registrado con el fin de llevar una trazabilidad.
- Se debe garantizar la oportuna erradicación de las amenazas. Para esto se debe actuar de manera correctiva pero también tomar las medidas para que el incidente no vuelva a presentarse.
- Debe existir una metodología que permita tratar los incidentes de manera preventiva y correctiva de acuerdo con su naturaleza.
- Debe existir una matriz de comunicaciones y responsabilidades para la gestión de los incidentes de seguridad informática.
- Es importante que las lecciones aprendidas sean registradas y aplicadas.
- Teniendo en cuenta que con mucha frecuencia se evidencian nuevas amenazas y herramientas tecnológicas, es indispensable mantener actualizado el proceso, herramienta, documentos y personal encargado de la seguridad.

18. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La organización debe identificar y gestionar proactivamente potenciales riesgos y los impactos que éstos podrían tener sobre las operaciones críticas del negocio; y actuar diligentemente frente a una situación de crisis o emergencia, recuperando los servicios ofrecidos a nuestros clientes en el menor tiempo posible, dentro de nuestras capacidades. Por tal razón se debe:

- Gestionar proactivamente los riesgos
- Establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis,
- Realizar una planificación estratégica para asegurar la continuidad del negocio en situaciones de crisis.
- Se deben establecer, documentar e implementar procesos y controles para asegurar el nivel de continuidad requerido para a seguridad de la información durante una situación adversa.
- Los controles de continuidad de deben evaluar periódicamente para validar su eficacia dentro de situaciones adversas.

- En lo posible, implementar redundancia en los sistemas de procesamiento.
- Las Comunicaciones en eventos de crisis deben estar previamente establecidas y documentada.
- Se deben realizar capacitaciones a los usuarios a fin de prepararlos para los incidentes, y también lleva a cabo pruebas regulares utilizando diferentes escenarios de sucesos.

19. CUMPLIMIENTO

La organización debe establecer mecanismos que permitan el cumplimiento de lo establecido en la presente política. Así como también, los requisitos legales y contractuales en lo referente a la seguridad de la información. El incumplimiento de lo establecido podrá resultar en la toma de acciones disciplinarias de acuerdo a la gravedad de la falta.

19.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

La organización debe implementar controles que permitan garantizar el cumplimiento con las políticas, normas y legislación aplicable enfocándose principalmente en lo que se refiere a seguridad de la información.

- Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar, documentar explícitamente y mantenerlos actualizados para cada sistema de información de la organización.
- Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
- Los registros se deben proteger contra pérdida, destrucción. Falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
- Se deben asegurar la privacidad y la protección de la información de datos personales como se exige en la legislación y la reglamentación pertinentes cuando sea necesario.
- Cuando se requiera se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentaciones pertinentes.
- Se deben establecer procedimientos que garanticen el uso del software de acuerdo a los términos previstos en la Ley de Propiedad Intelectual.
- Se debe comunicar a todos los colaboradores y proveedores acerca de la política de uso legal de software y sobre las consecuencias de la violación de la misma.

19.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

- La gestión de la seguridad de la información y su implementación se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
- Los líderes de área deben revisar con regularidad el cumplimiento del procesamiento y el procedimiento de seguridad de la información dentro de sus áreas de responsabilidad con las políticas, normas apropiadas y cualquier otro requisito de seguridad.
- Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento de las políticas y normas de seguridad de la información.
- Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo a su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.
- Una vez identificadas las vulnerabilidades, la organización deberá aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección

de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

19.3. VIGENCIA DE LA POLITICA

La presente Política de Seguridad de la Información entra en vigencia una vez sea oficializada y socializada a todo el personal de la OCBP.

Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se le deberá entregar una copia del presente documento y hacer firmar una declaración de toma de conocimiento y aceptación de la misma.

La presente política está alineada con las directrices de las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al responsable de este documento.

19.4. GESTIÓN DE EXCEPCIONES

Cualquier excepción a la presente Política de Seguridad de la Información deberá ser registrada e informada al departamento de Sistemas de la OCBP. Estas excepciones serán analizadas para evaluar el riesgo que podría introducir a la organización y, basados en la categorización de estos riesgos y previa autorización de la Gerencia se procederá o no a aceptar la petición de la excepción.

19.5. SANCIONES DISCIPLINARIAS

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno la OCBP. Es responsabilidad de todos los empleados, contratistas y terceros de la organización notificar al departamento de Sistemas de cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.