PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUCION UNIVERSITARIA DIGITAL DE ANTIOQUIA

.

CESAR ALEXANDER ZAPATA JIMENEZ
Coordinador de Infraestructura tecnológica

T (574) 219 83 32 ext. 8376
D Cll 10Sur # 50E - 31, sede Posgrados UdeA.

Contenido

INTRODUCCION

La gestión de los riesgos tecnológicos son aquellos procedimientos que reducen sustancialmente eventualidades que generan pérdidas en la información y blinda esencialmente aquellas plataformas y sistemas que la conservan, esta gestión permite conocer las debilidades que afectan durante todo el ciclo de vida el servicio.

Es fundamental contar con un plan de gestión de riesgos para garantizar la seguridad de la información. Por este motivo, surge la necesidad de expandir un análisis de riesgo de seguridad de la información, enfocado en la Institución Universitaria Digital de Antioquia (IU Digital). Para cumplir exitosamente con este plan se llevará a cabo el diagnóstico del sistema. Esto permitirá identificar la situación actual de la organización y las amenazas enfocadas en los activos de la información, logrando de esta manera un alto grado de satisfacción con la caracterización de riesgos existentes y las recomendaciones para la protección necesaria del sistema, parte del plan de gestión de riesgos en la seguridad de la información.

La contribución que proyecta este plan permite identificar el nivel de riesgo en que se hallan los activos de la información mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

OBJETIVOS

Objetivo General

- Desplegar un plan de gestión de políticas y normas de seguridad que permita reducir los riesgos de pérdida de activos de la información en la IU Digital.

Objetivos Específicos

- Tratar con eficiencia y buena gestión los eventos de seguridad de la información.
- Definir los principales activos a proteger en la IU Digital.
- Identificar todas las amenazas que afectan los activos de información.
- Establecer el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Minimizar los riesgos a los que están expuestos los activos de información.
- establecer procedimientos de reportes de incidencias a presentar en la IU Digital para su posterior tratamiento.

- Implementar un sistema de trazabilidad que permita evidenciar el cambio del nivel de riesgo actual con el impacto generado después de implementar un plan de gestión de seguridad de la información

ALCANCES

- Asignar roles de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión del riesgo en la seguridad de la información.
- Cumplir satisfactoriamente con la responsabilidad de la IU Digital para iniciar la implementación del plan de gestión del riesgo en la seguridad de la información.
- Capacitar todo el talento humano de la institución en el proceso de implementación del plan de gestión del riesgo de la seguridad de la información.

DEFINICIONES

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la IUDIGITAL y, en consecuencia, debe ser protegido.
Acuerdo de Confidencialidad: Es un documento en los que los funcionarios de la IUDIGITAL o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información del mismo, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.
Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
Capacity Planning: Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.
Centros de cableado: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
Custodio del activo de información: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
Guías de clasificación de la información: Directrices para catalogar la información de la IUDIGITAL y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.
Hacking ético: Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.
Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).
Integridad: Es la protección de la exactitud y estado completo de los activos.
Inventario de activos de información: Es una lista ordenada y documentada de los activos de información pertenecientes a la entidad.
Licencia de software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
Perfiles de usuario: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
Propiedad intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.
Propietario de la información: Es la unidad organizacional o proceso donde se crean los activos de información.
Recursos tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la IUDIGITAL.
Registros de Auditoría: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la IUDIGITAL. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
Responsable por el activo de información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
SGSI: Sistema de Gestión de Seguridad de la Información.
Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la entidad o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.
Sistemas de control ambiental: Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.
Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
Vulnerabilidades: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la entidad (amenazas), las cuales se constituyen en fuentes de riesgo.

LIMITACIONES

- Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la IU Digital.

GESTIÓN DE RIESGOS

Importancia de la gestión del riesgo

En el entorno corporativo se está haciendo mucho énfasis en salvar, proteger y custodiar el activo de la información, debido a que avances tecnológicos y plataformas de información están siendo implementados en todos los mercados del mundo.

Los riesgos por catástrofes naturales, riesgos relacionados con procedimientos inadecuados en el manejo de información, desconocimiento de normas y políticas de seguridad, son los aspectos más frecuentes y de alto impacto en las organizaciones. No tener un plan de gestión de riesgos es el mayor peligro para la pérdida de información.

La IU Digital, tiene como marco de referencia todos los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno digital que viene promoviendo actividades en el sector público, con el fin de ajustar modelos y estándares que permitan brindar seguridad a la información, dando cumplimiento de esta manera al Decreto 1078 de 2015.

Todos los sectores corporativos se encuentran implementando planes para reducir los riesgos que afectan todo el conjunto de herramientas tecnológicas que procesan los activos de información, considerando que en la actualidad los riesgos más comunes son generados por ataques implícitos que se dirigen a las plataformas corporativas, afectando la disponibilidad, seguridad e integridad de la información tratada y procesada por dispositivos tecnológicos.

Estas son las razones que activan las alarmas para estar preparados y prevenir todo tipo de arremetidas o catástrofes, ya que cuando el precio de rescate sobrepasa al costo de prevención, sin duda alguna, es más factible contar con planes implementados de gestión de riesgos que garanticen la alta disponibilidad, seguridad e integridad de la información, tras sufrir alguna pérdida o daño.

Considerando el estado actual de la IU Digital y para reducir todo tipo de peligros, es indispensable diseñar, desarrollar e implementar un plan de riesgos, que de fe de las buenas prácticas relacionadas con las normas y políticas de seguridad que certifican la alta disponibilidad y seguridad en los servicios.

DEFINICION GESTIÓN DEL RIESGO

La gestión del riesgo es el proceso de identificar, analizar y responder a factores de riesgo a lo largo de la vida de un proyecto y en beneficio de sus objetivos. La gestión de riesgos adecuada implica el control de posibles eventos futuros. Además, es proactiva, en lugar de reactiva. La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”.

IDENTIFICACIÓN DEL RIESGO

Riesgos de Imagen: Se relaciona con la confianza y la percepción por parte de la ciudadanía hacia la institución.

Riesgos Financieros: Se relacionan con el manejo de los pagos, la elaboración de los estados financieros, manejos de excedentes de tesorería, los recursos de la IUDIGITAL que incluyen: la ejecución presupuestal y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se relacionan con la capacidad para cumplir con los requisitos de ética pública, contractuales, legales, compromiso con la comunidad acorde a las funciones asignadas.

Riesgo Estratégico: Se relaciona con la forma en que se administra la institución. Son orientados a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la IUDIGITAL por parte de la alta gerencia.

Riesgos de Tecnología: Están asociados con la capacidad tecnológica que garantiza dar cumplimiento a las necesidades informáticas, que apoyan los procesos y procedimientos orientados a dar cumplimiento a la misión, visión y políticas institucionales.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional.

SITUACION NO DESEADA

- Secuestro de información.
- Daños en la información.
- Daño de dispositivos contenedores de información.
- Retrasos en la emisión de datos.
- Retrasos en asistencia técnica.
- Modificación en los accesos.
- Escape de información.
- Empleo indebido de información
- Incendio en la infraestructura física de la institución por catástrofes naturales.
- Incendios provocados en la infraestructura física de la institución.

ORIGEN DEL PLAN DE GESTION

Debido a que la IU Digital es una institución que se encuentra dando sus primeros pasos, al igual que su Dirección Tecnológica, se evidenció que existen diseños en los procesos muy básicos asignados a dicha dependencia entre otras debilidades que se encontraron en el procedimiento actual, por esta razón se hace necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.

El estado actual del sistema de seguridad de la información en la institución se encuentra planteado en el Diagnóstico de seguridad y privacidad de la Información emitido el 5 de julio de 2019.

El gobierno nacional o en su defecto el ministerio de las TIC ha protegido los proyectos que permiten conocer el trabajo de las entidades gubernamentales. Lo anterior hace necesario que la IU Digital efectúe los requisitos precisos para emitir la información de manera oportuna y eficiente a estas entidades, a la población y a la misma Institución.

PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

Brindar apoyo al modelo de seguridad y privacidad de la información de la IU Digital, garantizar aprobación legal y evidencias de la debida identificación, contar con un plan de contingencias a incidentes, describir los requisitos de seguridad para los activos de

información, organizar los procesos de gestión de riesgos en la seguridad de la información.

IDENTIFICACIÓN DEL RIESGO

Para entrar en la identificación del riesgo transitaremos por siete etapas fundamentales: Inicialmente se Identificarán los procesos, posteriormente identificaremos sus objetivos, una vez identificados sus objetivos pasaremos a la etapa de caracterización de activos de acuerdo con el proceso en estudio, teniendo ya identificado los activos se realizará un análisis de riesgos de acuerdo a las a causas, amenazas y vulnerabilidades, etapa por la que pasaremos en el proceso de identificación, una vez definamos los riesgos haremos una descripción de estos y posteriormente identificaremos los efectos de la materialización del riesgo.

ANALISIS DE VULNERABILIDADES

DESCRIPCIÓN DE VULNERABILIDADES

No obstante, a pesar de que los activos de la información se ven amenazados continuamente por error humano. En la IU Digital se encontraron otras amenazas e impactos como son:

- La red de internet implementada no es la más adecuada teniendo en cuenta que la mayor parte de la IU Digital tiene conexión WiFi y la señal se torna débil o no llega a algunas oficinas. Debido a que la infraestructura física es amplia, compleja y la señal debe atravesar paredes. El internet lento y la pérdida de señal afecta de forma directa los tiempos de producción laboral y desempeño de las funciones.

- Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad. No existe una estructura o protocolo fijo y establecido para la infraestructura física de IU Digital.

- Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.

- Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:
- Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.

- En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.
- En algunas secretarias de IU Digital no existen los equipos de cómputo suficientes para el uso de la totalidad de su personal. Existe un riesgo de pérdida de información ya que deben compartir los recursos informáticos.
- El Datacenter de la IUDIGITAL requiere de algunas características importantes para cumplir con las normas de funcionamiento (alimentación eléctrica estabilizada e ininterrumpida, sistemas contra incendios, control de acceso, extintores, sistemas de cámaras de vigilancia, alarmas contra incendios, control de temperatura y humedad, piso falso entre otros).
- No existen cuentas de usuario y claves para el acceso de los recursos informáticos, en equipos compartidos.
- La información es llevada en memorias o discos duros portátiles personales, por ende la información sale de la IUDIGITAL.
- No hay control para el uso de memorias portátiles en los equipos de IU Digital, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
- Se identificó un completo desconocimiento del tema de seguridad y privacidad de la información en IU Digital.
- No existe un Firewall para la red inalámbrica de IU Digital, solo existe uno dedicado para los servidores de las Secretarías de Hacienda y el Banco.
- No existe un área de sistemas con personal encargado de revisar, documentar, diseñar y controlar los procesos propios de un modelo de seguridad de la información para la IU Digital.
- No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la entidad.
- Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a pérdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.
- No existen procesos de copias de seguridad establecidos. Las copias de seguridad se están realizando únicamente en las secretarías y/o equipos donde se manejan software o sistemas de Información con un servidor dedicado a dicho propósito.
- No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la IU Digital. (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores)
- No se cuentan con los tipos de extintores adecuados para cada emergencia.
- La IU Digital cuenta con una planta de energía que en la actualidad no está funcionando, se han presentado cortes de energía suspendiendo los procesos laborales de todas las oficinas.

PROPUESTA DE SEGURIDAD

- Cambiar la red inalámbrica actual por cableado estructurado, para minimizar el problema de internet lento y caídas de señal.
- Implementar un firewall para todo el sistema de seguridad perimetral para la red que se utiliza en la IUDIGITAL.
- Socializar las políticas de seguridad y privacidad de la información con el personal de la IUDIGITAL.
- Creación de cuentas de usuario y claves para tratar de mitigar los riesgos de pérdida de información en manos de otro funcionario que use el equipo compartido.
- El personal de tecnología puede crear las cuentas y claves, socializando al personal de la IUDIGITAL la creación de claves en forma correcta.
- Crear un rubro del presupuesto para la adquisición de la licencia del sistema ofimático Office para los equipos de la IUDIGITAL.
- Implementar el sistema de documentación digital en la IUDIGITAL para reducir riesgos de pérdida de información física.
- La IUDIGITAL comprometida con la campaña cero papel está próxima en habilitar el software para digitalización de documentos y gestión documental en los próximos meses

PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

- Adquirir un servidor o servicio con características específicas para el almacenamiento de copias de seguridad de la información local manejada en las diferentes áreas.
- Adquirir servicios en la nube para la información de la IUDIGITAL con el fin de tener un respaldo en caso de accidentes en los servidores.
- Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso de que ocurran incidentes graves.
- Nunca se debe olvidar que la realidad es que la entidad puede sufrir un incidente que afecte su continuidad y dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves. Siempre teniendo en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Una de las principales características que debe poseer la entidad es buscar cómo establecer un Sistema de seguridad enfocado por procesos, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas, cuyo propósito se encamine a mitigar los riesgos encontrados.

PLAN DE CONTINUIDAD DEL NEGOCIO

- Diseñar un formato de chequeo de acuerdo con las necesidades de la organización que permita realizar auditorías periódicas con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.
- Socializar con los directivos, secretaría general y la dirección tecnológica la importancia del Plan de Continuidad de Negocio, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.
- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.
- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

    - Detectar el riesgo
    - Plantear controles y efectuar las implementaciones respectivas.
    - Mitigar el riesgo.
    - Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo con lo siguiente:

        - Política de copia de seguridad de datos
        - Procedimientos de almacenamiento fuera de la IUDIGITAL
        - Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones

PLAN DE CAPACITACIÓN

- Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:

    - Detectar los requerimientos tecnológicos
    - Determinar objetivos de capacitación para personal
    - Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.
    - Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la IUDIGITAL.
    - Evaluar los resultados de cada actividad.

PLAN DE TRANSICIÓN DE IPV4 A IPV6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existente actualmente por la IPv6 debido a que los equipos informáticos de la IUDIGITAL soportan la nueva versión del protocolo IP.

POLITICAS Y NORMAS

De acuerdo al análisis ejecutado con el fin de identificar todos los riesgos que surgen a partir de unas vulnerabilidades y unas amenazas se crean unas políticas y normas dirigidas para todas las partes interesadas en el tratamiento de información institucional.

POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

En la IUDIGITAL la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad. Consciente de las necesidades actuales, la entidad implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes. Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la IUDIGITAL, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información. La Política Global de Seguridad de la Información de la IUDIGITAL se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la IUDIGITAL. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control basados en la norma internacional ISO 27001:2013. El Comité de Seguridad tendrá la potestad de modificar la Política Global o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de estas.

POLITICA PARA USO DE DISPOSITIVOS MOVILES

La entidad proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios de la IUDIGITAL. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

Normas para uso de dispositivos móviles Normas dirigidas a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por la entidad.
- La Dirección de Tecnología debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la entidad.
- La Dirección de Tecnología debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- La Dirección de Tecnología debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- La Dirección de Tecnología debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- La Dirección de Tecnología debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales de la IUDIGITAL; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.
- La Dirección de Tecnología debe instalar un software de antivirus tanto en los dispositivos móviles institucionales. Como en los personales que hagan uso de los servicios provistos por la Entidad.
- La Dirección de Tecnología debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.
- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

POLITICA PARA USO DE CONEXIONES REMOTAS

La entidad establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la IUDIGITAL; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

Normas para uso de conexiones remotas Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología, debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la IUDIGITAL.

La Dirección de Tecnología debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la IUDIGITAL.

La Dirección de Tecnología debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

La Dirección de Tecnología debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la IUDIGITAL de manera permanente.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

La Oficina de Control Interno debe, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica de la IUDIGITAL.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la IUDIGITAL y deben acatar las condiciones de uso establecidas para dichas conexiones.

Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y en ninguna circunstancia, en computadores público, de hoteles o cafés internet, entre otros.

POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

La entidad como propietario de la información física así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma. La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad de la IUDIGITAL, son activos de la institución y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos del negocio. Toda la información sensible de la IUDIGITAL, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la . Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

Normas de responsabilidad por los activos Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Las Direcciones y Oficinas Asesoras de la IUDIGITAL, deben actuar como propietarias de la información física y electrónica de la IUDIGITAL, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.

Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.

Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la IUDIGITAL se encuentran sujetos a auditorías por parte de la Oficina de Control Interno y a revisiones de cumplimiento por parte de la dirección tecnológica.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la IUDIGITAL y, en consecuencia, debe asegurar su apropiada operación y administración.
La Dirección de Tecnología, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la IUDIGITAL.

La Dirección de Tecnología debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

La Dirección de Tecnología es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de estas.

La Dirección de Tecnología es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando les es formalmente solicitado.

Normas dirigidas a: TODOS LOS USUARIOS

Los recursos tecnológicos de la IUDIGITAL, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la IUDIGITAL.

Los recursos tecnológicos de la IUDIGITAL provistos a funcionarios y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las labores de la IUDIGITAL; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

Los funcionarios no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.

Los funcionarios no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la IUDIGITAL.

Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo al Director o Jefe de Oficina o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

La entidad definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de esta la cataloguen y determinen los controles requeridos para su protección. Toda la información de la IUDIGITAL debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas en la dirección tecnológica. Una vez clasificada la información, la entidad proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de esta, con el fin de promover el uso adecuado por parte de los funcionarios de la IUDIGITAL y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

Normas para la clasificación y manejo de la información Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.

La Dirección de Tecnología debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los propietarios de los activos de información deben clasificar su información de acuerdo con la guías de clasificación de la Información establecida.

Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física institucional.

La información física y digital de la IUDIGITAL debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

POLÍTICA DE USO DE PERIFERICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la IUDIGITAL será reglamentado por la Dirección de Tecnología, considerando las labores realizadas por los funcionarios y su necesidad de uso.

Normas uso de periféricos y medios de almacenamiento Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la IUDIGITAL.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la IUDIGITAL, de acuerdo con los lineamientos y condiciones establecidas.

La Dirección de Tecnología debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la IUDIGITAL, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

Normas dirigidas a: TODOS LOS USUARIOS

Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.

Los funcionarios de la IUDIGITAL y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.

Los funcionarios y personal provisto por terceras partes son responsables por la custodio de los medios de almacenamiento institucionales asignados.

Los funcionarios y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de la IUDIGITAL.

POLÍTICAS DE CONTROL DE ACCESO
POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

La Dirección de Tecnología, como responsables de las redes de datos y los recursos de red de la IUDIGITAL, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Normas de acceso a redes y recursos de red
Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la IUDIGITAL.

La Dirección de Tecnología debe asegurar que las redes inalámbricas de la IUDIGITAL cuenten con métodos de autenticación que evite accesos no autorizados.

La Dirección de Tecnología, debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la IUDIGITAL, así como velar por la aceptación de las responsabilidades de dicho terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

Normas dirigidas a: TODOS LOS USUARIOS

Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la IUDIGITAL, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la IUDIGITAL deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

La entidad establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la IUDIGITAL. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

Normas de administración de acceso de usuarios
Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la IUDIGITAL, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

La Dirección de Tecnología, previa solicitud de los Jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los sistemas de información como de la , debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.

La Dirección de Tecnología, debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la IUDIGITAL; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

La Dirección de Tecnología debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

La Dirección de Tecnología debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

Es responsabilidad de los Propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con la dirección tecnológica, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

Los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

Normas dirigidas a: DIRECTORES Y JEFES DE OFICINA

Los Directores y Jefes de Oficina deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los funcionarios que laboran en sus áreas, acogiéndose al procedimiento establecidos para tal fin.

POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información de la IUDIGITAL realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

Normas de responsabilidades de acceso de los usuarios Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la IUDIGITAL deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.

Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la IUDIGITAL deben acogerse a lineamientos para la configuración de contraseñas implantados por la entidad.

POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACION

La Dirección de Tecnología de la IUDIGITAL velará porque los recursos de la plataforma tecnológica y los servicios de red de la IUDIGITAL sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichas plataforma y servicios.

Normas de uso de altos privilegios y utilitarios de administración Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.

La Dirección de Tecnología debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

La Dirección de Tecnología debe verificar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.

La Dirección de Tecnología debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

La Dirección de Tecnología debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

La Dirección de Tecnología debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

Los administradores de los recursos tecnológicos y servicios de red, funcionarios de la Dirección de Tecnología, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica de la IUDIGITAL.

Los administradores de los recursos tecnológicos deben deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.

La Dirección de Tecnología debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

Las Direcciones o Jefaturas de áreas como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada. La Dirección de Tecnología, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Normas de control de acceso a sistemas y aplicativos
Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de la IUDIGITAL.

La Dirección de Tecnología debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

La Dirección de Tecnología debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

La Dirección de Tecnología debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

La Dirección de Tecnología debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.

Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

Los desarrolladores deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

POLÍTICAS DE CRIPTOGRAFIA
POLÍTICA DE CONTROLES CRIPTOGRAFICOS

La entidad velará porque la información de la IUDIGITAL, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

Normas de controles criptográficos Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

La Dirección de Tecnología debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.

La Dirección de Tecnología debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.

La Dirección de Tecnología, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

Los desarrolladores deben asegurarse de que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Dirección de Tecnología.

POLÍTICAS DE SEGURIDAD FISICA Y MEDIOAMBIENTAL
POLÍTICA DE AREAS SEGURAS

La entidad proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en su sede. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Normas de áreas seguras
Normas dirigidas a: DIRECCION DE TECNOLOGIA

Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de la Dirección de Tecnología autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.

La Dirección de Tecnología debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

La Dirección de Tecnología debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

La Dirección de Tecnología debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica

ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

La Dirección de Tecnología debe velar porque los recursos de la plataforma tecnológica de la IUDIGITAL ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

La Dirección de Tecnología debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

La Dirección de Tecnología debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: DIRECTORES Y JEFES DE AREA

Los directores y jefes de área que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su áreas.

Los directores y jefes de área que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.

Los directores y Jefes de Oficina deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios de la IUDIGITAL.

Normas dirigidas a: INFRAESTRUCTURA

El área de INFRAESTRUCTURA debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la IUDIGITAL.

El área de INFRAESTRUCTURA debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la IUDIGITAL.

El área de INFRAESTRUCTURA debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la IUDIGITAL.

El área de INFRAESTRUCTURA debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.

El área de INFRAESTRUCTURA debe controlar el ingreso de los visitantes a los centros de cableado que están bajo su custodia.

El área de INFRAESTRUCTURA debe cerciorarse de que los centros de cableado que están bajo su custodia se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

El área de INFRAESTRUCTURA, con el acompañamiento de la Dirección de Tecnología, debe verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.

Normas dirigidas a: TODOS LOS USUARIOS

Los ingresos y egresos de personal a las instalaciones de la IUDIGITAL deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la IUDIGITAL; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

Los funcionarios de la IUDIGITAL y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

La entidad para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la IUDIGITAL que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Normas de seguridad para los equipos institucionales Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la IUDIGITAL.

La Dirección de Tecnología debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la IUDIGITAL.

La Dirección de Tecnología, en conjunto con la Coordinación de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.

La Dirección de Tecnología debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la IUDIGITAL y configurar dichos equipos acogiendo los estándares generados.

La Dirección de Tecnología debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la IUDIGITAL y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

La Dirección de Tecnología debe aislar los equipos de áreas sensibles, como el área financiera para proteger su acceso de los demás funcionarios de la red de la empresa.

La Dirección de Tecnología debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la IUDIGITAL, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

La Oficina de Control Interno tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de la IUDIGITAL.

Normas dirigidas a: área de INFRAESTRUCTURA

El área de INFRAESTRUCTURA debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.

El área de INFRAESTRUCTURA debe restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.

El área de INFRAESTRUCTURA debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones

de la IUDIGITAL cuente con la autorización documentada y aprobada previamente por el Coordinador de bienes.

El área de INFRAESTRUCTURA debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la IUDIGITAL posean pólizas de seguro.

Normas dirigidas a: TODOS LOS USUARIOS

La Dirección de Tecnología es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la IUDIGITAL.

Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione la Dirección de Tecnología.

Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la IUDIGITAL el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior de la Dirección de Tecnología, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la IUDIGITAL, solo puede ser realizado por los funcionarios de la Dirección de Tecnología, o personal de terceras partes autorizado por dicha dirección.

Los funcionarios de la IUDIGITAL y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

Los funcionarios de la IUDIGITAL y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

En caso de pérdida o robo de un equipo de cómputo de la IUDIGITAL, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

Los funcionarios de la IUDIGITAL y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

POLITICAS DE SEGURIDAD EN LAS OPERACIONES
POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La Dirección de Tecnología, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de la IUDIGITAL, asignará funciones específicas a sus funcionarios, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos serán adecuadamente controlados y debidamente autorizados.

La Dirección de Tecnología proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la IUDIGITAL, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

Normas de asignación de responsabilidades operativas Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la IUDIGITAL.

La Dirección de Tecnología debe proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la IUDIGITAL.

La Dirección de Tecnología debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

La Dirección de Tecnología, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

La entidad proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

Normas de protección frente a software malicioso
Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la IUDIGITAL y los servicios que se ejecutan en la misma.

La Dirección de Tecnología debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

La Dirección de Tecnología debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

La Dirección de Tecnología, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

La Dirección de Tecnología, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la Dirección de Tecnología; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que a través de ella, la Dirección de Tecnología tome las medidas de control correspondientes.

POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La entidad certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la Dirección de Tecnología, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información. Así mismo, la entidad velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

Normas de copias de respaldo de la

información Normas dirigidas a: DIRECCION DE

TECNOLOGIA

La Dirección de Tecnología, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad. La Dirección de Tecnología debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

La Dirección de Tecnología, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

La Dirección de Tecnología debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

La Dirección de Tecnología debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la IUDIGITAL.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con la Dirección de Tecnología, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: TODOS LOS USUARIOS

Es responsabilidad de los usuarios de la plataforma tecnológica de la IUDIGITAL identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

La entidad realizará monitoreo permanente del uso que dan los funcionarios y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información de la IUDIGITAL. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros. La Dirección de Tecnología definirá la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos misionales de la IUDIGITAL.

Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de la IUDIGITAL.

La Dirección de Tecnología, deben definir de manera mensual cuáles monitoreos se realizarán de los registros de auditoría sobre los aplicativos donde se opera los procesos misionales de la

IUDIGITAL. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado.

La Dirección de Tecnología, a través de sus funcionarios, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.

La Dirección de Tecnología debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de la IUDIGITAL. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.

Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la Dirección de Tecnología.

Los desarrolladores deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoria que brinden información adicional a la estrictamente requerida.

POLITICA DE CONTROL AL SOFTWARE OPERATIVO

La entidad, a través de la Dirección de Tecnología, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

Normas de control al software operativo
Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la entidad.

La Dirección de Tecnología debe asegurarse que el software operativo instalado en la plataforma tecnológica de la IUDIGITAL cuenta con soporte de los proveedores.

La Dirección de Tecnología debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.

La Dirección de Tecnología debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

La Dirección de Tecnología debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la IUDIGITAL.

POLÍTICA DE GESTIÓN DE VULNERABILIDADES

La entidad, a través de la Dirección de tecnología, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la Plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

La Dirección de tecnología debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.

La Dirección de tecnología debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.

La Dirección de Tecnología, a través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

la Dirección de tecnología, debe revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES
POLÍTICA DE GESTION Y ASEGURAMIENTO DE LAS REDES DE DATOS

La entidad establecerá, a través de la Dirección de Tecnología, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos. De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la IUDIGITAL.

Normas de gestión y aseguramiento de las redes de datos Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la IUDIGITAL.

La Dirección de Tecnología debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

La Dirección de Tecnología debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para el instituto.

La Dirección de Tecnología debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

La Dirección de Tecnología debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la IUDIGITAL, acogiendo buenas prácticas de configuración segura.

La Dirección de Tecnología, a través de sus funcionarios, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la entidad en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

La Dirección de Tecnología debe instalar protección entre las redes internas de la IUDIGITAL y cualquier red externa, que este fuera de la capacidad de control y administración de la IUDIGITAL.

La Dirección de Tecnología debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la IUDIGITAL.

POLÍTICA DE USO DEL CORREO ELECTRONICO

La entidad, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Normas de uso del correo electrónico
Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.

La Dirección de Tecnología debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

La Dirección de Tecnología debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.

La Dirección de Tecnología debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

La Dirección de Tecnología junto con la oficina de comunicaciones debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la IUDIGITAL o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.

Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la IUDIGITAL. El correo institucional no debe ser utilizado para actividades personales.

Los mensajes y la información contenida en los buzones de correo son propiedad de la IUDIGITAL y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

Los usuarios de correo electrónico institucional tienen prohibido el envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la IUDIGITAL y el personal provisto por terceras partes.

No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la entidad y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

POLÍTICA DE USO ADECUADO DE INTERNET

La entidad consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en el instituto.

Normas de uso adecuado de internet Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

La Dirección de Tecnología debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

La Dirección de Tecnología debe monitorear continuamente el canal o canales del servicio de Internet.

La Dirección de Tecnología debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

La Dirección de Tecnología debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios del servicio de Internet de la IUDIGITAL deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

No está permitido el intercambio no autorizado de información de propiedad de la IUDIGITAL, de sus clientes y/o de sus funcionarios, con terceros.

POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

La entidad asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La Entidad propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

Normas de intercambio de información

Para procesos de contratación se debe establecer con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios de la IUDIGITAL que les ha sido entregada en razón del cumplimiento de los objetivos misionales de la IUDIGITAL.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

Los propietarios de los activos de información deben velar porque la información de la IUDIGITAL o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

Los propietarios de los activos de información deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.

Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

Los propietarios de los activos de información deben autorizar los requerimientos de solicitud/envío de información de la IUDIGITAL por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

Los propietarios de los activos de información deben asegurarse que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de la IUDIGITAL así como del procedimiento de intercambio de información.

Los propietarios de los activos de información deben verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Normas dirigidas a: TODOS LOS USUARIOS:

Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la IUDIGITAL o de sus beneficiarios.

No está permitido el intercambio de información sensible de la IUDIGITAL por vía telefónica.

POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

La entidad asegurará que el software adquirido y desarrollado tanto al interior de la IUDIGITAL, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos. Las áreas propietarias de sistemas de información y la Dirección de Tecnología incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN, DIRECCION DE TECNOLOGIA

Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de la IUDIGITAL formalmente asignada.

La Dirección de Tecnología debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

Las áreas propietarias de los sistemas de información, en acompañamiento con la Dirección de Tecnología deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.

Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.

Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.

Los desarrolladores deben atender los protocolos sugeridos por la Dirección de Tecnología en los aplicativos desarrollados.

POLÍTICA DE DESARROLLO SEGURO, REALIZACION DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

La entidad velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado.

Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la IUDIGITAL.

Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN

Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe implantar 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.

La Dirección de Tecnología debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la IUDIGITAL.

La Dirección de Tecnología debe asegurase 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.

La Dirección de Tecnología debe generar 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

La Dirección de Tecnología, a través de sus funcionarios, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

La Dirección de Tecnología debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la IUDIGITAL.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de la IUDIGITAL; dicho soporte debe contemplar tiempos de respuesta aceptables.

Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.

Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.

Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

POLÍTICA PARA LA PROTECCION DE LOS DATOS DE PRUEBA

La Dirección de Tecnología de la IUDIGITAL protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

Normas para la protección de los datos de prueba Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.

La Dirección de Tecnología debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

La entidad promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas. De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad. La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

Normas para el reporte y tratamiento de incidentes de seguridad Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los propietarios de los activos de información deben informar los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.
Normas dirigidas a: DIRECCIÓN DE TECNOLOGIA

La dirección de tecnología debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Normas dirigidas a: TODOS LOS USUARIOS

Es responsabilidad de los funcionarios de la IUDIGITAL y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo a la Oficina de Riesgo para que se registre y se le dé el trámite necesario.

POLÍTICAS DE INCLUSION DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACION

La entidad proporcionará los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación. Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. La entidad mantendrá canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología, debe elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

La Dirección de Tecnología debe participar activamente en las pruebas de recuperación ante desastres y notificar los resultados al Comité Gobierno Digital.

Normas dirigidas a: DIRECTORES Y JEFES DE OFICINA

Los Directores y Jefes de Oficina deben identificar al interior de sus áreas y generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

POLÍTICA DE REDUNDANCIA

La entidad propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la IUDIGITAL

Normas de redundancia Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la entidad y la plataforma tecnológica que los apoya.

La Dirección de Tecnología debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la IUDIGITAL.

La Dirección de Tecnología, a través de sus funcionarios, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la IUDIGITAL.

POLÍTICAS DE CUMPLIMIENTO
POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

La entidad velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

Normas de cumplimiento con requisitos legales y contractuales Normas dirigidas a: OFICINA ASESORA JURIDICA

La Oficina Asesora Jurídica y debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la entidad y relacionados con seguridad de la información.

Normas dirigidas a: DIRECCIÓN DE TECNOLOGIA

La Dirección de Tecnología debe certificar que todo el software que se ejecuta en la entidad esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

La Dirección de Tecnología debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la IUDIGITAL para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la entidad propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información. Se establecerán los términos, condiciones y finalidades para las cuales la entidad, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la IUDIGITAL, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la entidad exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la IUDIGITAL y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Normas de privacidad y protección de datos personales
Normas dirigidas a: AREAS QUE PROCESAN DATOS PERSONALES

Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la IUDIGITAL.

Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas, delegadas para el tratamiento de dichos datos personales.

Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: DIRECCIÓN DE TECNOLOGIA

La Dirección de Tecnología debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la IUDIGITAL o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Normas dirigidas a: USUARIOS DE LOS PORTALES DE LA IUDIGITAL

Los usuarios de los portales de la IUDIGITAL deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.

Los usuarios de los portales de la IUDIGITAL deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales de la IUDIGITAL.

Los usuarios de los portales de la IUDIGITAL deben aceptar el suministro de datos personales que pueda hacer la entidad a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoría interna o externa.

CONCLUSIONES

El seguimiento constante a los procesos y la implementación del plan de mitigación de riesgo de seguridad de la información deben ser ejecutados, monitoreados y actualizados frecuentemente.

Es indispensable implementar el plan de gestión de riesgo que permitirá prevenir las posibles amenazas encontradas en la infraestructura tecnológica de la IUDIGITAL.

Las políticas de seguridad de la información de la IUDIGITAL deben ser revisadas y actualizadas conforme al crecimiento, cambios de la estructura organizacional, exigencias del gobierno y los mismos procesos dentro de la IUDIGITAL de Antioquia