El futuro es de todos

Mininterior

Sistema de Gestión de Seguridad de la Información - SGSI

Unidad Nacional de Protección

Fecha: Noviembre 2021

UNIDAD NACIONAL DE PROTECCIÓN

Sistema de Gestión de Seguridad de la Información - SGSI

Riesgos de Seguridad digital

Fecha: Noviembre 2021

SEGURIDAD DE LA INFORMACION

Seguridad de la Información

Seguridad Informática

Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida o daño de información, acceso a bases de datos por personas no autorizadas .

Seguridad de la Información

Es el conjunto de recursos y técnicas que permitan resguardar y proteger la información garantizando la confidencialidad, disponibilidad e integridad de la misma.

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética

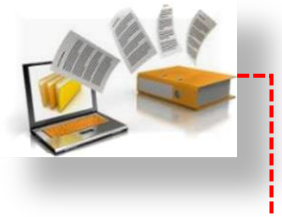
La ciberseguridad busca proteger la información digital en los sistemas interconectados. Está comprendida dentro de la seguridad de la información

SEGURIDAD DE LA INFORMACION

En términos prácticos

SEGURIDAD DE LA INFORMACION – GESTIÓN DE RIESGOS

Matriz de activos identificados y valorados



Contexto → Identificación de activos → Identificación de riesgos → Valoración impacto

Valoración impacto → Valoración probabilidad → Riesgo Inherente → Identificación de controles → Valoración del control

Valoración del control → Riesgo Residual → Plan de Tratamiento

SEGURIDAD DE LA INFORMACION

¿QUÉ ES UN ACTIVO DE INFORMACIÓN?

Es cualquier bien tangible o intangible en el que se procese, almacene y/o gestione información, y tenga valor para la UNP.

La información la encontramos disponible a través de diferentes medios, como:

Almacenada en computadores y servidores

Impresa o escrita en papel

Transmitida en medios electrónicos

Almacenada en USB, Discos duros externos Smartphone.....

MEDIO ORAL

SEGURIDAD DE LA INFORMACION

SEGURIDAD DE LA INFORMACION

SEGURIDAD DE LA INFORMACION

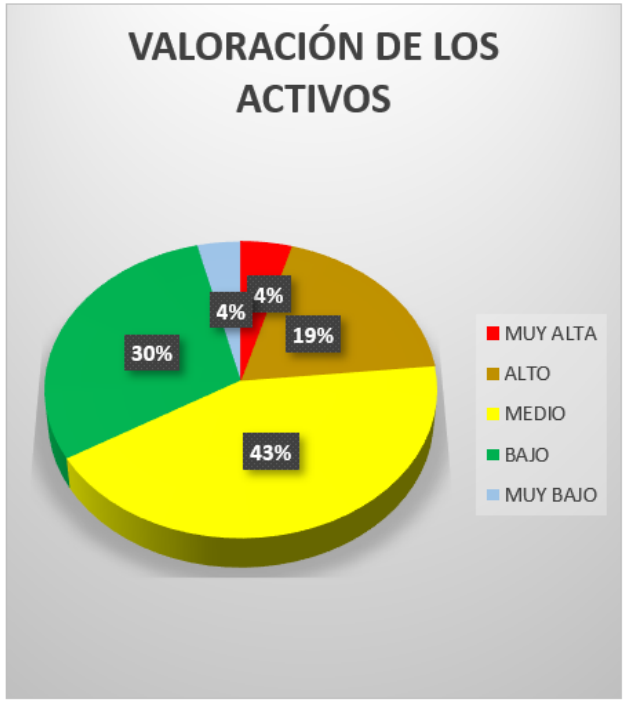
Que debemos proteger

SEGURIDAD DE LA INFORMACION

2.1 IDENTIFICACIÓN DEL				REDES		INSTALACIONES				PERSONAL		MEDIO DE CONSERVACIÓN			PROCEDIMENTAL Y ESTRCUTURAL		OTROS SERVICIOS EXTERNOS					2.4. VALORACIÓN DE LOS ACTIVOS								
																						NORMATIVIDAD				ATRIBUTOS DE LA (TRIADA)				
PROCESO	NOMBRE DE LA DEPENDENCIA	NOMBRE DEL GRUPO INTERNO DE TRABAJO	TIP(	Local	Red Publica	Data Center	Archivo Central	Archivo de Gestión	Sitio Externo	Personal Interno	Personal Externo	Físico	Digital	Personas	Politicas	Procedimientos	ALMACENAMIENTO EXTERNO DISCO DUROS, UBS, MCS, CD, DVD	COMPUTADORES PERSONALES / CAFE INTERNET	ALMACENAMIENTO EN LA NUBE EXTERNA (DROP BOX, GOOGLE DRIVE)	CORREO EXTERNOS (GMAIL, HOTMAIL, YAHOO)	USO DE APLICACIONES DE TERCEROS (WTRANFER, WHASAP,)	Ley 1581 de 2012 (Datos Personales)	Ley 1712 de 2014 (Ley de transparencia)	Servicios esenciales	Infraestrcutura critica	Confidencialidad	Integridad	Disponibilidad	CID O TRIADA	V. CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN
Gestión Control Disciplinario Interno	SECRETARIA_GENERAL	Grupo de Control Disciplinario Interno (GCDI)	DATOS (info	X			X	X		X		X			X	X					SI	SI		N/A	MA	MA	MA	MA	SENSIBLE (Clasificada) Confidencial
Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Grupo Secretaría Técnica del Comité de Evaluación de Riesgo y Recomendación de Medidas (CERREM	DATOS (info	X		X	X	X		X		X	X		X	X	X					N/A	SI	Internet	N/A	A	A	A	A	SENSIBLE (Clasificada) Confidencial
Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Grupo de Solicitudes de Protección (GSP)	DATOS (info	X			X	X		X		X	X		X	X						SI	SI	Red	N/A	M	A	M	M	SENSIBLE (Clasificada) Confidencial
Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Implementación (GI)	DATOS (info	X			X	X		X	X	X	X	X	X	X		X	X			SI	SI	Internet	N/A	MA	MA	MB	M	SENSIBLE (Clasificada) Confidencial
Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Implementación (GI)	DATOS (info	X			X	X		X	X	X	X	X	X	X		X	X			SI	SI	Internet	N/A	MA	MA	MB	M	SENSIBLE (Clasificada) Confidencial
Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Implementación (GI)	DATOS (info	X			X	X		X	X		X		X	X			X			SI	SI	Internet	N/A	MA	MA	MB	M	SENSIBLE (Clasificada) Confidencial
Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Implementación (GI)	DATOS (info	X			X	X		X		X	X	X	X	X			X			SI	SI	SIGOB	N/A	MA	MA	MB	M	SENSIBLE (Clasificada) Confidencial

Levantamiento de Activos de Información

VALORACIÓN DE LOS ACTIVOS	No. de Activos	
MUY ALTA	90	15%
ALTO	155	25%
MEDIO	183	30%
BAJO	184	30%
MUY BAJO	8	1%
Total	620	



CLASIFICACION DE LA	No. de Activos
RESERVADA	31
SENSIBLE	233
INTERNA	217
PUBLICA	139
Total	620

Levantamiento de Activos de Información

ACTIVOS DE INFORMACIÓN
INFORMACIÓN SENSIBLE - CONFIDENCIAL - (CLASIFICADA)

MACRO PROCESO	PROCESO	NOMBRE DE LA DEPENDENCIA	NOMBRE DEL GRUPO INTERNO DE TRABAJO	233
MISIONAL	Gestión Especializada de Seguridad y Protección	SUBDIRECCION_ESPECIALIZADA_DE_SEGURIDAD_Y_PROTECCIÓN	Grupo de Recepción, Ánalisis, evaluación de riesgos y recomendaciones (GRAERR)	38
ESTRATEGICO	Gestión Estratégica del Talento Humano	SUBDIRECCION_DE_TALENTO_HUMANO	Grupo de Registro y Control (GRC)	31
MISIONAL	Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Grupo Cuerpo Técnico de Recopilación y Análisis de Información (CTRAI)	23
MISIONAL	Gestión Especializada de Seguridad y Protección	SUBDIRECCION_ESPECIALIZADA_DE_SEGURIDAD_Y_PROTECCIÓN	Grupo Cuerpo de Seguridad y Protección (GCSP)	16
EVALUACION_Y_CONTROL	Gestión Especializada de Seguridad y Protección	SUBDIRECCION_ESPECIALIZADA_DE_SEGURIDAD_Y_PROTECCIÓN	Grupo de Automotores (GA)	15
ESTRATEGICO	Gestión Estratégica del Talento Humano	SUBDIRECCION_DE_TALENTO_HUMANO	Grupo de Capacitación, Bienestar y Salud en el Trabajo (GBSST)	14
MISIONAL	Gestión Especializada de Seguridad y Protección	DIRECCION_GENERAL	Subdirección Especializada de Seguridad y Protección	12
APOYO	Gestión Control Disciplinario Interno	SECRETARIA_GENERAL	Grupo de Control Disciplinario Interno (GCDI)	11
ESTRATEGICO	Gestión Estratégica del Talento Humano	SUBDIRECCION_DE_TALENTO_HUMANO	Grupo de Nómina (GN)	10
MISIONAL	Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Grupo Secretaría Técnica del Comité de Evaluación de Riesgo y Recomendación de Medidas (CERREM	8
MISIONAL	Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Implementación (GI)	8
MISIONAL	Gestión Especializada de Seguridad y Protección	SUBDIRECCION_ESPECIALIZADA_DE_SEGURIDAD_Y_PROTECCIÓN	Grupo de Gestión de Viáticos y Desplazamientos (GGVT)	8
ESTRATEGICO	Sistema de Gestión	DIRECCION_GENERAL	Oficna Asesora de Planeación e Información	7
APOYO	Gestión Financiera	SECRETARIA_GENERAL	Grupo de Tesorería (GT)	6
MISIONAL	Gestión Especializada de Seguridad y Protección	SUBDIRECCION_ESPECIALIZADA_DE_SEGURIDAD_Y_PROTECCIÓN	Grupo de Planeación y Seguimiento (GPS)	6
MISIONAL	Gestión Especializada de Seguridad y Protección	SUBDIRECCION_ESPECIALIZADA_DE_SEGURIDAD_Y_PROTECCIÓN	Grupo de Enlace con Talento Humano (GETH)	5
ESTRATEGICO	Direccionamiento Estratégico	DIRECCION_GENERAL	Direccion General	2
MISIONAL	Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Grupo de Solicitudes de Protección (GSP)	2
MISIONAL	Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Hombres de Protección (GHP)	2
MISIONAL	Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Control de Desplazamientos Esquemas Protectivos (GCDEP)	1
MISIONAL	Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Grupo de Solicitudes de Protección (GSP)	1
MISIONAL	Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Subdirección de Evaluación de Riesgo	1
MISIONAL	Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Grupo de Valoración Preliminar - GVP	1
MISIONAL	Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Grupo Control de Asignacioes de emisiones de Trabajo (GCAET)	1
MISIONAL	Gestión Medidas de Protección	SUBDIRECCION_DE_TALENTO_HUMANO	Grupo de Selección y Evaluación (GES)	1
MISIONAL	Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Seguridad Especial (GSE)	1
MISIONAL	Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Apoyo y Reentrenamiento Operativo (GARO)	1
MISIONAL	Gestión Medidas de Protección	SUBDIRECCION_DE_PROTECCION	Grupo de Vehiculos de Protección (GRVP)	1

Levantamiento de Activos de Información

ACTIVOS DE INFORMACIÓN
INFORMACIÓN ALTAMENTE CONFIDENCIAL - (RESERVADA)

MACRO PROCESO	PROCESO	NOMBRE DE LA DEPENDENCIA	NOMBRE DEL GRUPO INTERNO DE TRABAJO	31
MISIONAL	Gestión Especializada de Seguridad y Protección	SUBDIRECCION_ESPECIALIZADA_DE_SEGURIDAD_Y_PROTECCIÓN	Grupo de Implementación, supervisión y finalización de medidas (GISFM)	21
MISIONAL	Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Subdirección de Evaluación de Riesgo	4
MISIONAL	Gestión Especializada de Seguridad y Protección	SUBDIRECCION_ESPECIALIZADA_DE_SEGURIDAD_Y_PROTECCIÓN	Grupo de Planeación y Seguimiento (GPS)	3
MISIONAL	Gestión Evaluación del Riesgo	SUBDIRECCION_DE_EVALUACION_DEL_RIESGO	Grupo Cuerpo Técnico de Recopilación y Análisis de Información (CTRAI)	2
MISIONAL	Gestión Especializada de Seguridad y Protección	SUBDIRECCION_ESPECIALIZADA_DE_SEGURIDAD_Y_PROTECCIÓN	Grupo de Automotores (GA)	1

SEGURIDAD DE LA INFORMACION

Riesgos	CAUSAS	CONSECUENCIAS
Posibilidad de comprometer la integridad de la información institucional debido a fallas técnicas y operativas en el proceso.	* (Proceso) Asignación errada de los derechos de acceso *(Tecnología) Ausencia de mecanismos de identificación y autentificación * (Proceso) Ausencia de control de los activos que se encuentran fuera de las instalaciones * (Tecnologia) Mantemiento insuficiente * (Proceso) Exposición de datos de respaldo * (Tecnologia) Ausencia de mecanismos de monitoreo * (Tecnologia) Ausencia de manuales de uso * (Tecnologia) Mantemiento insuficiente	* Inconsistencias en la calidad de la información. * Afectación en la comunicación de los servicios. * Inadecuada toma de decisiones. * Perdida reputacional. * Alteración de la información para beneficio propio.
Posibilidad de comprometer la confidencialidad de la información institucional debido a fallas técnicas y operativas en el proceso.	*(Personal) Trabajo de personal externo o de mantenimiento no supervisado. *(Procesos) Carencia de procedimientos adecuados de reutilización de medios, computadores y disposición final de medio de almacenamiento (Físico y digital). *(Procesos) Desconocimiento o falta de capacitación en seguridad de la información *(Procesos) Equipos de cómputo desatendidos *(Procesos) Errores en la definición de roles en las aplicaciones.	*Fuga de información * Imagen y reputación de la entidad * Incumplimiento normativo. * Sanciones por los entes de control. * Afectación en las finanzas de la entidad. * Afectación en la credibilidad hacia la entidad. * Compromiso en la cadena de suministros que afecta la promesa de valor de la entidad.
Posibilidad de comprometer la disponibilidad por dependencia (parcial o total) tecnológica de los proveedores de servicios TICS	*(Tecnología) Dependencia tecnológica de los proveedores de las herramientas. *(Tecnología) Limitada capacidad de respuesta frente a eventualidades, urgencias, incidencias y requerimientos por parte de TICS *(Procesos) Debilidad en la socialización de las actualizaciones a los sistemas *(Financieros) Limitada asignación de recursos presupuestales para la ejecución de los planes asociados al proceso Posibilidad de pérdida de los registros documentales que no están en los repositorios no institucionales, o en los PC´s de los funcionarios	*No poder responder oportuna y eficazmente a las solicitudes que presentan las partes interesadas de la entidad. *Reprocesos en la gestión *Dificultad en el acceso a la información por indisponibilidad del servicio.

SEGURIDAD DE LA INFORMACION

Riesgos	CAUSAS	CONSECUENCIAS
Posibilidad de no atender las necesidades de automatización de los procesos de la entidad, debido a capacidad limitada de los productos adquiridos	*(Tecnología) Los proveedores son los dueños del código fuente de los aplicativos, y del conocimiento de los mismos; si para continuidad del negocio necesariamente se les debe contratar porque son los únicos que pueden dar soporte y mantenimiento por fallos del mismo, y/o actualizaciones requeridas al producto *(Tecnología) Algunos servicios Tic que soportan la operación de la entidad son especializados y no se cuenta con las capacidades para atenderlos adecuadamente, por lo que se tercerizan *(Tecnología) Contratación de productos TICS con especificaciones generales frente a las necesidades puntuales de la entidad, evidenciado en el momento de entrega de los mismos.	*Interrupción total o parcia del negocio por fallos en los sistemas de información esenciales, y en los recursos y servicios TIC *Sobrecostos en los productos y servicios contratados por la entidad.
Posibilidad de tener Sistemas de información desatendidos o sin soporte debido a la imposibilidad de continuidad a los contratos de soporte y mantenimiento	*(Tecnología) El fabricante del sistema de información está sancionado para contratar con entidades del Estado *(Financieros) Falta de recurso para dar continuidad a contratos de soporte y mantenimiento	*Imagen y reputación de la entidad *Incumplimiento normativo. *Sanciones por los entes de control. *Afectación en las finanzas de la entidad. *Afectación en la credibilidad hacia la entidad. *Compromiso en la cadena de suministros que afecta la promesa de valor de la entidad.
Posibilidad de afectacion de integridad, confidencilaid y/o disponibilidad de la informacion por errores humanos	Desconocimiento de los lineamientos del SGSI (politicas, normas y procedimientos). Ausencia de personal que cumpla con los Roles establecidos en la guía de roles de Servicios Tecnológicos de la Estrategia de gobierno en Linea. Falta de uso y apropiacion en cultura organizacional en seguridad de la informacion. Abuso de derechos Destruccion de equipos o medios Copia no autorizada de información Modificación no aupotrizada de informacion. Ausencia de personal. Uso no autorizado de equipos Exceso de confianza	* Fuga de informacion * Inconsistencias en la calidad de la información. * Afectación en la comunicación de los servicios. * Inadecuada toma de decisiones. * Perdida reputacional. * Alteración de la información para beneficio propio.

SEGURIDAD DE LA INFORMACION

IDENTIFICACIÓN							
COMPONENTE DEL SIG	TIPO DE PROCESO	PROCESO	OBJETIVO DEL PROCESO	RIESGO	CAUSAS O EVENTOS	TIPO DE RIESGO	CONSECUENCIAS (RESULTADO DEL EVENTO)
Sistema de Gestión de Seguridad de Información (SGSI)	Proceso_Estratégico	Gestión Estratégica del Talento Humano	Gestionar, vincular y promover el desarrollo y bienestar del talento humano que permita contribuir al logro de la misionalidad de la entidad, en el marco de la integridad y del servicio público.	**Posibilidad de comprometer la integridad de la información institucional debido a fallas técnicas y operativas en el proceso.**	* (Proceso) Asignación errada de los derechos de acceso *(Tecnologia) Ausencia de mecanismos de identificación y autentificación * (Proceso) Ausencia de control de los activos que se encuentran fuera de las instalaciones * (Tecnologia) Mantemiento insuficiente * (Proceso) Exposición de datos de respaldo * (Tecnologia) Ausencia de mecanismos de monitoreo * (Tecnologia) Ausencia de manuales de uso * (Tecnologia) Mantemiento insuficiente *(Procesos) Modificar la información sin autorización Inadecuado manejo de la información causada por una indebida manipulación de los custodios *(Procesos) Acceso no autorizado la información. *(Tecnologia) Inconsistencias en la información *(Personal) Errores humanos *(Procesos) Errores en la definición de roles en las aplicaciones *(Procesos) Debilidad en la capacitación *(Procesos) actualización a los usuarios en el manejo de las aplicaciones, sistemas de información y herramientas *(Procesos) Debilidad en la documentación sobre el uso de los servicios tecnológicos *(Procesos) Falta de planes de sensibilización en SI *(Procesos) Inadecuado control de acceso lógico y fisico a los activos de información. *(Personal) Hurto de equipos *(Procesos) Falta de divulgación de las políticas y procedimientos propios del proceso	Seguridad Digital	

SEGURIDAD DE LA INFORMACION

	CALIFICACIÓN				
CONSECUENCIAS (RESULTADO DEL EVENTO)	PROBABILIDAD ESCALA RARA VEZ = 1 IMPROBABLE = 2 POSIBLE = 3 PROBABLE = 4 CASI SEGURO = 5	IMPACTO ESCALA INSIGNIFICANTE = 3 MENOR = 6 MODERADO = 9 MAYOR = 12 CATASTROFICO = 15	EVALUACION DEL RIESGO INHERENTE (PROBABILIDAD X IMPACTO)	NIVEL DE RIESGO INHERENTE (RIESGOS PROPIOS DEL PROCESO O ACTIVIDAD)	CONTROLES EXISTENTES (SE DETALLAN LOS CONTROLES EXISTENTE)
* Inconsistencias en la calidad de la información y reprocesos. * Afectación en la comunicación de los servicios. * Perdida reputacional. * Incumplimiento normativo * Procesos administrativos y/o judiciales	4	12	48	EXTREMO	1. Políticas de Seguridad. 2. Autenticacion de usuarios 3.Perfiles de usuario 4.Uso aceptable de activos 5. Informacion documentada (procedimientos, guias etc.)

SEGURIDAD DE LA INFORMACION

VALORACIÓN

CANT. DE CONTROLES EXISTENTES (SE SUMAN LOS # DE CONTROLES EXISTENTES REFIERE COLUMNA N)	TIPO DE CONTROL 1= INEXISTENTE 2= DETECTIVO 3= CORRECTIVO 4= PREVENTIVO	PERIODICIDAD DEL CONTROL 1= OCASIONAL 2= PERIÓDICO 3= PERMANENTE	PRODUCTO (TIPO DE CONTROL X PERIODICIDAD DEL CONTROL)	EFICACIA DEL CONTROL	VALORACION DEL CONTROL (EFICACIA DEL CONTROL EN TÉRMINOS CUALITATIVOS)	GRADO DE EXPOSICIÓN (RESIDUAL) (EVALUACIÓN DEL RIESGO INHERENTE / EFICACIA DE CONTROL)	NIVEL DE RIESGO RESIDUAL ESCALA EXTREMO ALTO MODERADO BAJO
6	2	3	6	3	MEDIO	4,0	BAJO

SEGURIDAD DE LA INFORMACION

PLAN DE TRATAMIENTO

OPCIÓN DE TRATAMIENTO (MITIGAR /ASUMIR /EVITAR / /TRASNFERIR)	ACCIONES (CONTROL EFECTIVO FUTURO A IMPLEMENTAR) (DETALLAR PLAN DE ACCIÓN EN TÉRMINOS DEL CICLO PVHA)	RESPONSABLE (DEL TRATAMIENTO DEL RIESGO)	CRONOGRAMA DEL PLAN DE ACCIÓN	
			FECHA INICIO (dd/mm/aaaa)	FECHA FIN (dd/mm/aaaa)
	P: Se Pleanea realizar reunion con partes interesadas. H: Se toman decisiones mediante un plan de sesnibilización para los servidores publicos y contratista referente al cumplimiento de politicas. Elabore un instrumento de evaliuación frente a los temas sensibilizados. V: aplico instrumento y evaluo mediante indicadres de sesibilizacion. A: Se realizan memorando a todo el personal indicando que se lean las politicas y las aplique porque el resultado de la evaluacion no fue optima y se detecta que hay falencias en la apropiacion de las mismas.		P: H: V: A:	P: H: V: A:

artesanías de colombia

La seguridad de la información no es un producto

Es un proceso

Es un compromiso de TODOS

David Yacel Espinosa Vanegas
CISO – Oficial de Seguridad de la Información
david.espinosa@unp.gov.co

artesanías
de colombia

Trabajo en equipo